Chapter 1

Strong Customer Authentication and Common and Secure Methods of Communication

Chapter -1 Guidance

1. Payment services offered electronically should be carried out in a secure manner, adopting technologies able to guarantee the safe authentication of the user and to reduce, to the maximum extent possible, the risk of fraud. The authentication procedure should include, in general, transaction monitoring mechanisms to detect attempts to use a payment service user's personalised security credentials that were lost, stolen, or misappropriated and should also ensure that the payment service user is the legitimate user and therefore is giving consent for the transfer of funds and access to its account information through a normal use of the personalised security credentials. Furthermore, it is necessary to specify the requirements of the strong customer authentication that should be applied each time a payer accesses its payment account online, initiates an electronic payment transaction or carries out any action through a remote channel which may imply a risk of payment fraud or other abuse, by requiring the generation of an authentication code which should be resistant against the risk of being forged in its entirety or by disclosure of any of the elements upon which the code was generated.

2. As fraud methods are constantly changing, the requirements of strong customer authentication should allow for innovation in the technical solutions addressing the emergence of new threats to the security of electronic payments. To ensure that the requirements to be laid down are effectively implemented on a continuous basis, it is also appropriate to require that the security measures for the application of strong customer authentication and its exemptions, the measures to protect confidentiality and integrity of the personalised security credentials, and the measures establishing common and secure open standards of communication are documented, periodically tested, evaluated and audited by auditors with expertise in IT security and payments, and operationally independent. In order to allow the FCA to monitor the quality of the review of these measures, such reviews should be made available to the FCA upon its request.

3. As electronic remote payment transactions are subject to a higher risk of fraud, it is necessary to introduce additional requirements for the strong customer authentication of such transactions, ensuring that the elements dynamically link the transaction to an amount and a payee specified by the payer when initiating the transaction.

4. Dynamic linking is possible through the generation of authentication codes, which are subject to a set of strict security requirements. To remain technologically neutral, a specific technology for the implementation of authentication codes should not be required. Therefore authentication codes should be based on solutions such as generating and validating one-time passwords, digital signatures or other cryptographically underpinned validity assertions using keys or cryptographic material stored in the authentication elements, as long as the security requirements are fulfilled.

5. It is necessary to lay down specific requirements for the situation where the final amount is not known at the moment the payer initiates an electronic remote payment transaction, in order to ensure that the strong customer authentication is specific to the maximum amount that the payer has given consent for as referred to in the Payment Services Regulations 2017 (SI 2017/752).

6. In order to ensure the application of strong customer authentication, it is also necessary to require adequate security features for the elements of strong customer authentication categorised as knowledge (something only the user knows), such as length or complexity, for the elements categorised as possession (something only the user possesses),

such as algorithm specifications, key length and information entropy, and for the devices and software that read elements categorised as inherence (something the user is), such as algorithm specifications, and biometric sensor and template protection features, in particular to mitigate the risk that those elements are uncovered, disclosed to and used by unauthorised parties. It is also necessary to lay down the requirements to ensure that those elements are independent, so that the breach of one does not compromise the reliability of the others, in particular when any of these elements are used through a multi-purpose device, such as a tablet or a mobile phone which can be used both for giving the instruction to make the payment and in the authentication process.

7. The requirements of strong customer authentication apply to payments initiated by the payer, regardless of whether the payer is a natural person or a legal entity.

8. Due to their very nature, payments made through the use of an anonymous payment instrument are not subject to the obligation of strong customer authentication. Where the anonymity of such instruments is lifted on contractual or legislative grounds, payments are subject to the security requirements that follow from the Payment Services Regulations 2017 (SI 2017/752) and this Regulatory Technical Standard.

9. In accordance with the Payment Services Regulations 2017 (SI 2017/752), exemptions to the principle of strong customer authentication have been defined based on the level of risk, amount, recurrence and the payment channel used for the execution of the payment transaction.

10. Actions which imply access to the balance and the recent transactions of a payment account without disclosure of sensitive payment data, recurring payments to the same payees which have been previously set up or confirmed by the payer through the use of strong customer authentication, and payments to and from the same natural or legal person with accounts with the same payment service provider pose a low level of risk, thus allowing payment service providers not to apply strong customer authentication. This leaves aside that in accordance with Regulations 68, 69 and 70 of the Payment Services Regulations 2017 (SI 2017/752), payment initiation service providers, payment service providers issuing card-based payment instruments and account information service providers should only seek and obtain the necessary and essential information from the account servicing payment service provider for the provision of a given payment service with the consent of the payment service user. Such consent can be given individually for each request of information or for each payment to be initiated or, for account information service providers, as a mandate for designated payment accounts and associated payment transactions as established in the contractual agreement with the payment service user.

11. Exemptions for low-value contactless payments at points of sale, which also take into account a maximum number of consecutive transactions or a certain fixed maximum value of consecutive transactions without applying strong customer authentication, allow for the development of user-friendly and low-risk payment services and should therefore be provided for. It is also appropriate to establish an exemption for the case of electronic payment transactions initiated at unattended terminals, where the use of strong customer authentication may not always be easy to apply due to operational reasons (e.g. to avoid queues and potential accidents at toll gates or for other safety or security risks).

12. Similar to the exemption for low-value contactless payments at the point of sale, a proper balance needs to be struck between the interest in enhanced security in remote payments and the needs of user-friendliness and accessibility of payments in the area of e-commerce. In line with those principles, thresholds below which no strong customer authentication needs to be applied should be set in a prudent manner, to cover only online purchases of low value. The thresholds for online purchases should be set more prudently, considering that the fact that the person is not physically present when making the purchase poses a slightly higher security risk.

13. The requirements of strong customer authentication apply to payments initiated by the payer, regardless of whether the payer is a natural person or a legal entity. Many corporate payments are initiated through dedicated processes or protocols which guarantee the high levels of payment security that the Payment Services Regulations 2017 (SI 2017/752) aims to achieve through strong customer authentication. Where the FCA establishes that those payment processes and protocols that are only made available to payers who are not consumers achieve the objectives of the Payment Services Regulations 2017 (SI 2017/752) in terms of security, payment service providers may, in relation to those processes or protocols, be exempted from the strong customer authentication requirements.

14. In the case of real-time transaction risk analysis that categorises a payment transaction as low risk, it is also appropriate to introduce an exemption for the payment service provider that intends not to apply strong customer authentication through the adoption of effective and risk-based requirements which ensure the safety of the payment service user's funds and personal data. Those risk-based requirements should combine the scores of the risk analysis, confirming that no abnormal spending or behavioural pattern of the payer has been identified, taking into account other risk factors including information on the location of the payer and of the payee with monetary thresholds based on fraud rates calculated for remote payments. Where, on the basis of the real-time transaction risk analysis, a payment cannot be qualified as posing a low level of risk, the payment service provider should revert to strong customer authentication. The maximum value of such risk-based exemption should be set in a manner ensuring a very low corresponding fraud rate, also by comparison to the fraud rates of all the payment transactions of the payment service provider, including those authenticated through strong customer authentication, within a certain period of time and on a rolling basis.

15. For the purpose of ensuring an effective enforcement, payment service providers that wish to benefit from the exemptions from strong customer authentication should regularly monitor and make available to the FCA upon its request, for each payment transaction type, the value of fraudulent or unauthorised payment transactions and the observed fraud rates for all their payment transactions, whether authenticated through strong customer authentication or executed under a relevant exemption.

16. The collection of this new historical evidence on the fraud rates of electronic payment transactions will also contribute to an effective review by the FCA of the thresholds for an exemption to strong customer authentication based on a real-time transaction risk analysis. The FCA should review and, if appropriate, update these Standards, including where appropriate the thresholds and fraud rates, with the aim of enhancing the security of remote electronic payments, on a regular basis to take account of innovation and technical developments as well as other relevant matters.

17. Payment service providers that make use of any of the exemptions to be provided for should be allowed at any time to choose to apply strong customer authentication to the actions and to the payment transactions referred to in those provisions.

18. The measures that protect the confidentiality and integrity of personalised security credentials, as well as authentication devices and software, should limit the risks relating to fraud through unauthorised or fraudulent use of payment instruments and unauthorised access to payment accounts. To this end it is necessary to introduce requirements on the secure creation and delivery of the personalised security credentials and their association with the payment service user, and to provide conditions for the renewal and deactivation of those credentials.

19. In order to ensure effective and secure communication between the relevant actors in the context of account information services, payment initiation services and confirmation on the availability of funds, it is necessary to specify the requirements of common and secure open standards of communication to be met by all relevant payment service providers. The Payment Services Regulations 2017 (SI 2017/752) provide for the access and use of payment account information by account information service providers. These Standards therefore do not change the rules of access to accounts other than payment accounts.

20. Each account servicing payment service provider with payment accounts that are accessible online should offer at least one access interface enabling secure communication with account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. The interface should enable the account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments to identify themselves to the account servicing payment service provider. It should also allow account information service providers and payment initiation service providers to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user.

FCA 2021/45 To ensure technology and business model neutrality, the account servicing payment service providers should be free to decide whether to offer an interface that is dedicated to the communication with account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments, or to allow, for that communication, the use of the interface for the identification

and communication with the account servicing payment service providers' payment service users.

21. In order to allow account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments to develop their technical solutions, the technical specification of the interface should be adequately documented and made publicly available. The effect of Articles 30(3) and (5) is that the account servicing payment service provider should offer a facility enabling the payment service providers to test the technical solutions

at least six months prior to by FCA 2021/45 the date on which the interface will be launched to the market. To ensure the interoperability of different technological communication solutions, the interface should use standards of communication which are developed by international standardisation organisations.

22. The quality of the services provided by account information service providers and payment initiation service providers will depend on the proper functioning of the interfaces put in place or adapted by account servicing payment service providers. It is therefore important that in case of non-compliance of such interfaces with the provisions included in these Standards, measures are taken to guarantee business continuity for the benefit of the users of those services. It is the responsibility of the FCA to ensure that account information service providers and payment initiation service providers are not blocked or obstructed in the provision of their services.

23. Where access to payment accounts is offered by means of a dedicated interface, in order to ensure the right of payment service users to make use of payment initiation service providers and of services enabling access to account information, as provided for in the Payment Services Regulations 2017 (SI 2017/752), it is necessary to require that dedicated interfaces have the same level of availability and performance as the interface available to the payment service user. Account servicing payment service providers should also define transparent key performance indicators and service level targets for the availability and performance of dedicated interfaces that are at least as stringent as those for the interface used for their payment service users. Those interfaces should be tested by the payment service providers who will use them, and should be stress-tested and monitored by the FCA.

24. To ensure that payment service providers who rely on the dedicated interface can continue to provide their services in case of problems of availability or inadequate performance, it is necessary to provide, subject to strict conditions, a fallback mechanism that will allow such providers to use the interface that the account servicing payment service provider maintains for the identification of, and communication with, its own payment service users. Certain account servicing payment service providers will be exempted from having to provide such a fallback mechanism through their customer-facing interfaces where the FCA establishes that the dedicated interfaces comply with specific conditions that ensure unhampered competition. In the event that the exempted dedicated interfaces fail to comply with the required conditions, the granted exemptions shall be revoked by the FCA.

25. In order to allow the FCA to effectively supervise and monitor the implementation and management of the communication interfaces, the account servicing payment service providers should make a summary of the relevant documentation available on their website, and provide, upon request, the FCA with documentation of the solutions in case of emergencies. The account servicing payment service providers should also make publicly available the statistics on the availability and performance of that interface.

26. In order to safeguard the confidentiality and the integrity of data, it is necessary to ensure the security of communication sessions between account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. It is in particular necessary to require that secure encryption is applied between account information service providers, payment initiation service providers, payment service providers issuing card-based payment instruments and account servicing payment service providers when exchanging data.

27. To improve user confidence and ensure strong customer authentication, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall identify themselves to account servicing payment service providers using a form of identification issued by an independent third party. Where relevant, the use of electronic identification means and trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July

2014 on electronic identification and trust service for electronic transactions in the internal market, as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 as came into force on IP completion day as defined in the EU (Withdrawal Agreement) Act 2020, should be taken into account, in particular with regard to notified electronic identification schemes.

2. As fraud methods are constantly changing, the requirements of strong customer authentication should allow for innovation in the technical solutions addressing the emergence of new threats to the security of electronic payments. To ensure that the requirements to be laid down are effectively implemented on a continuous basis, it is also appropriate to require that the security measures for the application of strong customer authentication and its exemptions, the measures to protect confidentiality and integrity of the personalised security credentials, and the measures establishing common and secure open standards of communication are documented, periodically tested, evaluated and audited by auditors with expertise in IT security and payments, and operationally independent. In order to allow the FCA to monitor the quality of the review of these measures, such reviews should be made available to the FCA upon its request.

3. As electronic remote payment transactions are subject to a higher risk of fraud, it is necessary to introduce additional requirements for the strong customer authentication of such transactions, ensuring that the elements dynamically link the transaction to an amount and a payee specified by the payer when initiating the transaction.

4. Dynamic linking is possible through the generation of authentication codes, which are subject to a set of strict security requirements. To remain technologically neutral, a specific technology for the implementation of authentication codes should not be required. Therefore authentication codes should be based on solutions such as generating and validating one-time passwords, digital signatures or other cryptographically underpinned validity assertions using keys or cryptographic material stored in the authentication elements, as long as the security requirements are fulfilled.

5. It is necessary to lay down specific requirements for the situation where the final amount is not known at the moment the payer initiates an electronic remote payment transaction, in order to ensure that the strong customer authentication is specific to the maximum amount that the payer has given consent for as referred to in the Payment Services Regulations 2017 (SI 2017/752).

6. In order to ensure the application of strong customer authentication, it is also necessary to require adequate security features for the elements of strong customer authentication categorised as knowledge (something only the user knows), such as length or complexity, for the elements categorised as possession (something only the user possesses), such as algorithm specifications, key length and information entropy, and for the devices and software that read elements categorised as inherence (something the user is), such as algorithm specifications, and biometric sensor and template protection features, in particular to mitigate the risk that those elements are uncovered, disclosed to and used by unauthorised parties. It is also necessary to lay down the requirements to ensure that those elements are independent, so that the breach of one does not compromise the reliability of the others, in particular when any of these elements are used through a multi-purpose device, such as a tablet or a mobile phone which can be used both for giving the instruction to make the payment and in the authentication process.

7. The requirements of strong customer authentication apply to payments initiated by the payer, regardless of whether the payer is a natural person or a legal entity.

8. Due to their very nature, payments made through the use of an anonymous payment instrument are not subject to the obligation of strong customer authentication. Where the anonymity of such instruments is lifted on contractual or legislative grounds, payments are subject to the security requirements that follow from the Payment Services Regulations 2017 (SI 2017/752) and this Regulatory Technical Standard.

9. In accordance with the Payment Services Regulations 2017 (SI 2017/752), exemptions to the principle of strong customer authentication have been defined based on the level of risk, amount, recurrence and the payment channel used for the execution of the payment transaction.

10. Actions which imply access to the balance and the recent transactions of a payment account without disclosure of sensitive payment data, recurring payments to the same payees

which have been previously set up or confirmed by the payer through the use of strong customer authentication, and payments to and from the same natural or legal person with accounts with the same payment service provider pose a low level of risk, thus allowing payment service providers not to apply strong customer authentication. This leaves aside that in accordance with Regulations 68, 69 and 70 of the Payment Services Regulations 2017 (SI 2017/752), payment initiation service providers, payment service providers issuing card-based payment instruments and account information service providers should only seek and obtain the necessary and essential information from the account servicing payment service provider for the provision of a given payment service with the consent of the payment service user. Such consent can be given individually for each request of information or for each payment to be initiated or, for account information service providers, as a mandate for designated payment accounts and associated payment transactions as established in the contractual agreement with the payment service user.

11. Exemptions for low-value contactless payments at points of sale, which also take into account a maximum number of consecutive transactions or a certain fixed maximum value of consecutive transactions without applying strong customer authentication, allow for the development of user-friendly and low-risk payment services and should therefore be provided for. It is also appropriate to establish an exemption for the case of electronic payment transactions initiated at unattended terminals, where the use of strong customer authentication may not always be easy to apply due to operational reasons (e.g. to avoid queues and potential accidents at toll gates or for other safety or security risks).

12. Similar to the exemption for low-value contactless payments at the point of sale, a proper balance needs to be struck between the interest in enhanced security in remote payments and the needs of user-friendliness and accessibility of payments in the area of e-commerce. In line with those principles, thresholds below which no strong customer authentication needs to be applied should be set in a prudent manner, to cover only online purchases of low value. The thresholds for online purchases should be set more prudently, considering that the fact that the person is not physically present when making the purchase poses a slightly higher security risk.

13. The requirements of strong customer authentication apply to payments initiated by the payer, regardless of whether the payer is a natural person or a legal entity. Many corporate payments are initiated through dedicated processes or protocols which guarantee the high levels of payment security that the Payment Services Regulations 2017 (SI 2017/752) aims to achieve through strong customer authentication. Where the FCA establishes that those payment processes and protocols that are only made available to payers who are not consumers achieve the objectives of the Payment Services Regulations 2017 (SI 2017/752) in terms of security, payment service providers may, in relation to those processes or protocols, be exempted from the strong customer authentication requirements.

14. In the case of real-time transaction risk analysis that categorises a payment transaction as low risk, it is also appropriate to introduce an exemption for the payment service provider that intends not to apply strong customer authentication through the adoption of effective and risk-based requirements which ensure the safety of the payment service user's funds and personal data. Those risk-based requirements should combine the scores of the risk analysis, confirming that no abnormal spending or behavioural pattern of the payer has been identified, taking into account other risk factors including information on the location of the payer and of the payee with monetary thresholds based on fraud rates calculated for remote payments. Where, on the basis of the real-time transaction risk analysis, a payment cannot be qualified as posing a low level of risk, the payment service provider should revert to strong customer authentication. The maximum value of such risk-based exemption should be set in a manner ensuring a very low corresponding fraud rate, also by comparison to the fraud rates of all the payment transactions of the payment service provider, including those authenticated through strong customer authentication, within a certain period of time and on a rolling basis.

15. For the purpose of ensuring an effective enforcement, payment service providers that wish to benefit from the exemptions from strong customer authentication should regularly monitor and make available to the FCA upon its request, for each payment transaction type, the value of fraudulent or unauthorised payment transactions and the observed fraud rates for all their payment transactions, whether authenticated through strong customer authentication or executed under a relevant exemption.

16. The collection of this new historical evidence on the fraud rates of electronic payment transactions will also contribute to an effective review by the FCA of the thresholds for an exemption to strong customer authentication based on a real-time transaction risk analysis. The FCA should review and, if appropriate, update these Standards, including where appropriate the thresholds and fraud rates, with the aim of enhancing the security of remote electronic payments, on a regular basis to take account of innovation and technical developments as well as other relevant matters.

17. Payment service providers that make use of any of the exemptions to be provided for should be allowed at any time to choose to apply strong customer authentication to the actions and to the payment transactions referred to in those provisions.

18. The measures that protect the confidentiality and integrity of personalised security credentials, as well as authentication devices and software, should limit the risks relating to fraud through unauthorised or fraudulent use of payment instruments and unauthorised access to payment accounts. To this end it is necessary to introduce requirements on the secure creation and delivery of the personalised security credentials and their association with the payment service user, and to provide conditions for the renewal and deactivation of those credentials.

19. In order to ensure effective and secure communication between the relevant actors in the context of account information services, payment initiation services and confirmation on the availability of funds, it is necessary to specify the requirements of common and secure open standards of communication to be met by all relevant payment service providers. The Payment Services Regulations 2017 (SI 2017/752) provide for the access and use of payment account information by account information service providers. These Standards therefore do not change the rules of access to accounts other than payment accounts.

20. Each account servicing payment service provider with payment accounts that are accessible online should offer at least one access interface enabling secure communication with account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. The interface should enable the account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments to identify themselves to the account servicing payment service provider. It should also allow account information service providers and payment initiation service providers to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user.

FCA 2021/45 To ensure technology and business model neutrality, the account servicing payment service providers should be free to decide whether to offer an interface that is dedicated to the communication with account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments, or to allow, for that communication, the use of the interface for the identification and communication with the account servicing payment service providers' payment service users.

21. In order to allow account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments to develop their technical solutions, the technical specification of the interface should be adequately documented and made publicly available. The effect of Articles 30(3) and (5) is that the account servicing payment service provider should offer a facility enabling the payment service providers to test the technical solutions

at least six months prior to by FCA 2021/45 the date on which the interface will be launched to the market. To ensure the interoperability of different technological communication solutions, the interface should use standards of communication which are developed by international standardisation organisations.

22. The quality of the services provided by account information service providers and payment initiation service providers will depend on the proper functioning of the interfaces put in place or adapted by account servicing payment service providers. It is therefore important that in case of non-compliance of such interfaces with the provisions included in these Standards, measures are taken to guarantee business continuity for the benefit of the users of those services. It is the responsibility of the FCA to ensure that account information service providers and payment initiation service providers are not blocked or obstructed in the provision of their services.

23. Where access to payment accounts is offered by means of a dedicated interface, in order to ensure the right of payment service users to make use of payment initiation service providers and of services enabling access to account information, as provided for in the Payment Services Regulations 2017 (SI 2017/752), it is necessary to require that dedicated interfaces have the same level of availability and performance as the interface available to the payment service user. Account servicing payment service providers should also define transparent key performance indicators and service level targets for the availability and performance of dedicated interfaces that are at least as stringent as those for the interface used for their payment service users. Those interfaces should be tested by the payment service providers who will use them, and should be stress-tested and monitored by the FCA.
24. To ensure that payment service providers who rely on the dedicated interface can continue to provide their services in case of problems of availability or inadequate performance, it is necessary to provide, subject to strict conditions, a fallback mechanism that will allow such providers to use the interface that the account servicing payment service provider maintains for the identification of, and communication with, its own payment service users. Certain account servicing payment service providers will be exempted from having to provide such a fallback mechanism through their customer-facing interfaces where the FCA establishes that the dedicated interfaces comply with specific conditions that ensure unhampered competition. In the event that the exempted dedicated interfaces fail to comply with the required conditions, the granted exemptions shall be revoked by the FCA.
25. In order to allow the FCA to effectively supervise and monitor the implementation and management of the communication interfaces, the account servicing payment service providers should make a summary of the relevant documentation available on their website, and provide, upon request, the FCA with documentation of the solutions in case of emergencies. The account servicing payment service providers should also make publicly available the statistics on the availability and performance of that interface.
26. In order to safeguard the confidentiality and the integrity of data, it is necessary to ensure the security of communication sessions between account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. It is in particular necessary to require that secure encryption is applied between account information service providers, payment initiation service providers, payment service providers issuing card-based payment instruments and account servicing payment service providers when exchanging data.
27. To improve user confidence and ensure strong customer authentication, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall identify themselves to account servicing payment service providers using a form of identification issued by an independent third party. Where relevant, the use of electronic identification means and trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust service for electronic transactions in the internal market, as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 as came into force on IP completion day as defined in the EU (Withdrawal Agreement) Act 2020, should be taken into account, in particular with regard to notified electronic identification schemes.

3. As electronic remote payment transactions are subject to a higher risk of fraud, it is necessary to introduce additional requirements for the strong customer authentication of such transactions, ensuring that the elements dynamically link the transaction to an amount and a payee specified by the payer when initiating the transaction.
4. Dynamic linking is possible through the generation of authentication codes, which are subject to a set of strict security requirements. To remain technologically neutral, a specific technology for the implementation of authentication codes should not be required. Therefore authentication codes should be based on solutions such as generating and validating one-time passwords, digital signatures or other cryptographically underpinned validity assertions using keys or cryptographic material stored in the authentication elements, as long as the security requirements are fulfilled.
5. It is necessary to lay down specific requirements for the situation where the final amount is not known at the moment the payer initiates an electronic remote payment transaction, in

1

order to ensure that the strong customer authentication is specific to the maximum amount that the payer has given consent for as referred to in the Payment Services Regulations 2017 (SI 2017/752).

6. In order to ensure the application of strong customer authentication, it is also necessary to require adequate security features for the elements of strong customer authentication categorised as knowledge (something only the user knows), such as length or complexity, for the elements categorised as possession (something only the user possesses), such as algorithm specifications, key length and information entropy, and for the devices and software that read elements categorised as inherence (something the user is), such as algorithm specifications, and biometric sensor and template protection features, in particular to mitigate the risk that those elements are uncovered, disclosed to and used by unauthorised parties. It is also necessary to lay down the requirements to ensure that those elements are independent, so that the breach of one does not compromise the reliability of the others, in particular when any of these elements are used through a multi-purpose device, such as a tablet or a mobile phone which can be used both for giving the instruction to make the payment and in the authentication process.

7. The requirements of strong customer authentication apply to payments initiated by the payer, regardless of whether the payer is a natural person or a legal entity.

8. Due to their very nature, payments made through the use of an anonymous payment instrument are not subject to the obligation of strong customer authentication. Where the anonymity of such instruments is lifted on contractual or legislative grounds, payments are subject to the security requirements that follow from the Payment Services Regulations 2017 (SI 2017/752) and this Regulatory Technical Standard.

9. In accordance with the Payment Services Regulations 2017 (SI 2017/752), exemptions to the principle of strong customer authentication have been defined based on the level of risk, amount, recurrence and the payment channel used for the execution of the payment transaction.

10. Actions which imply access to the balance and the recent transactions of a payment account without disclosure of sensitive payment data, recurring payments to the same payees which have been previously set up or confirmed by the payer through the use of strong customer authentication, and payments to and from the same natural or legal person with accounts with the same payment service provider pose a low level of risk, thus allowing payment service providers not to apply strong customer authentication. This leaves aside that in accordance with Regulations 68, 69 and 70 of the Payment Services Regulations 2017 (SI 2017/752), payment initiation service providers, payment service providers issuing card-based payment instruments and account information service providers should only seek and obtain the necessary and essential information from the account servicing payment service provider for the provision of a given payment service with the consent of the payment service user. Such consent can be given individually for each request of information or for each payment to be initiated or, for account information service providers, as a mandate for designated payment accounts and associated payment transactions as established in the contractual agreement with the payment service user.

11. Exemptions for low-value contactless payments at points of sale, which also take into account a maximum number of consecutive transactions or a certain fixed maximum value of consecutive transactions without applying strong customer authentication, allow for the development of user-friendly and low-risk payment services and should therefore be provided for. It is also appropriate to establish an exemption for the case of electronic payment transactions initiated at unattended terminals, where the use of strong customer authentication may not always be easy to apply due to operational reasons (e.g. to avoid queues and potential accidents at toll gates or for other safety or security risks).

12. Similar to the exemption for low-value contactless payments at the point of sale, a proper balance needs to be struck between the interest in enhanced security in remote payments and the needs of user-friendliness and accessibility of payments in the area of e-commerce. In line with those principles, thresholds below which no strong customer authentication needs to be applied should be set in a prudent manner, to cover only online purchases of low value. The thresholds for online purchases should be set more prudently, considering that the fact that the person is not physically present when making the purchase poses a slightly higher security risk.

13. The requirements of strong customer authentication apply to payments initiated by the payer, regardless of whether the payer is a natural person or a legal entity. Many corporate

payments are initiated through dedicated processes or protocols which guarantee the high levels of payment security that the Payment Services Regulations 2017 (SI 2017/752) aims to achieve through strong customer authentication. Where the FCA establishes that those payment processes and protocols that are only made available to payers who are not consumers achieve the objectives of the Payment Services Regulations 2017 (SI 2017/752) in terms of security, payment service providers may, in relation to those processes or protocols, be exempted from the strong customer authentication requirements.

14. In the case of real-time transaction risk analysis that categorises a payment transaction as low risk, it is also appropriate to introduce an exemption for the payment service provider that intends not to apply strong customer authentication through the adoption of effective and risk-based requirements which ensure the safety of the payment service user's funds and personal data. Those risk-based requirements should combine the scores of the risk analysis, confirming that no abnormal spending or behavioural pattern of the payer has been identified, taking into account other risk factors including information on the location of the payer and of the payee with monetary thresholds based on fraud rates calculated for remote payments. Where, on the basis of the real-time transaction risk analysis, a payment cannot be qualified as posing a low level of risk, the payment service provider should revert to strong customer authentication. The maximum value of such risk-based exemption should be set in a manner ensuring a very low corresponding fraud rate, also by comparison to the fraud rates of all the payment transactions of the payment service provider, including those authenticated through strong customer authentication, within a certain period of time and on a rolling basis.

15. For the purpose of ensuring an effective enforcement, payment service providers that wish to benefit from the exemptions from strong customer authentication should regularly monitor and make available to the FCA upon its request, for each payment transaction type, the value of fraudulent or unauthorised payment transactions and the observed fraud rates for all their payment transactions, whether authenticated through strong customer authentication or executed under a relevant exemption.

16. The collection of this new historical evidence on the fraud rates of electronic payment transactions will also contribute to an effective review by the FCA of the thresholds for an exemption to strong customer authentication based on a real-time transaction risk analysis. The FCA should review and, if appropriate, update these Standards, including where appropriate the thresholds and fraud rates, with the aim of enhancing the security of remote electronic payments, on a regular basis to take account of innovation and technical developments as well as other relevant matters.

17. Payment service providers that make use of any of the exemptions to be provided for should be allowed at any time to choose to apply strong customer authentication to the actions and to the payment transactions referred to in those provisions.

18. The measures that protect the confidentiality and integrity of personalised security credentials, as well as authentication devices and software, should limit the risks relating to fraud through unauthorised or fraudulent use of payment instruments and unauthorised access to payment accounts. To this end it is necessary to introduce requirements on the secure creation and delivery of the personalised security credentials and their association with the payment service user, and to provide conditions for the renewal and deactivation of those credentials.

19. In order to ensure effective and secure communication between the relevant actors in the context of account information services, payment initiation services and confirmation on the availability of funds, it is necessary to specify the requirements of common and secure open standards of communication to be met by all relevant payment service providers. The Payment Services Regulations 2017 (SI 2017/752) provide for the access and use of payment account information by account information service providers. These Standards therefore do not change the rules of access to accounts other than payment accounts.

20. Each account servicing payment service provider with payment accounts that are accessible online should offer at least one access interface enabling secure communication with account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. The interface should enable the account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments to identify themselves to the account servicing payment service provider. It should also allow account information service providers and payment initiation service providers to rely on the authentica-

1

tion procedures provided by the account servicing payment service provider to the payment service user.

FCA 2021/45 To ensure technology and business model neutrality, the account servicing payment service providers should be free to decide whether to offer an interface that is dedicated to the communication with account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments, or to allow, for that communication, the use of the interface for the identification and communication with the account servicing payment service providers' payment service users.

21. In order to allow account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments to develop their technical solutions, the technical specification of the interface should be adequately documented and made publicly available. The effect of Articles 30(3) and (5) is that the account servicing payment service provider should offer a facility enabling the payment service providers to test the technical solutions

at least six months prior to by FCA 2021/45 the date on which the interface will be launched to the market. To ensure the interoperability of different technological communication solutions, the interface should use standards of communication which are developed by international standardisation organisations.

22. The quality of the services provided by account information service providers and payment initiation service providers will depend on the proper functioning of the interfaces put in place or adapted by account servicing payment service providers. It is therefore important that in case of non-compliance of such interfaces with the provisions included in these Standards, measures are taken to guarantee business continuity for the benefit of the users of those services. It is the responsibility of the FCA to ensure that account information service providers and payment initiation service providers are not blocked or obstructed in the provision of their services.

23. Where access to payment accounts is offered by means of a dedicated interface, in order to ensure the right of payment service users to make use of payment initiation service providers and of services enabling access to account information, as provided for in the Payment Services Regulations 2017 (SI 2017/752), it is necessary to require that dedicated interfaces have the same level of availability and performance as the interface available to the payment service user. Account servicing payment service providers should also define transparent key performance indicators and service level targets for the availability and performance of dedicated interfaces that are at least as stringent as those for the interface used for their payment service users. Those interfaces should be tested by the payment service providers who will use them, and should be stress-tested and monitored by the FCA.

24. To ensure that payment service providers who rely on the dedicated interface can continue to provide their services in case of problems of availability or inadequate performance, it is necessary to provide, subject to strict conditions, a fallback mechanism that will allow such providers to use the interface that the account servicing payment service provider maintains for the identification of, and communication with, its own payment service users. Certain account servicing payment service providers will be exempted from having to provide such a fallback mechanism through their customer-facing interfaces where the FCA establishes that the dedicated interfaces comply with specific conditions that ensure unhampered competition. In the event that the exempted dedicated interfaces fail to comply with the required conditions, the granted exemptions shall be revoked by the FCA.

25. In order to allow the FCA to effectively supervise and monitor the implementation and management of the communication interfaces, the account servicing payment service providers should make a summary of the relevant documentation available on their website, and provide, upon request, the FCA with documentation of the solutions in case of emergencies. The account servicing payment service providers should also make publicly available the statistics on the availability and performance of that interface.

26. In order to safeguard the confidentiality and the integrity of data, it is necessary to ensure the security of communication sessions between account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. It is in particular necessary to require that secure encryption is applied between account information service providers, payment initiation service providers, payment service providers issuing card-

based payment instruments and account servicing payment service providers when exchanging data.

27. To improve user confidence and ensure strong customer authentication, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall identify themselves to account servicing payment service providers using a form of identification issued by an independent third party. Where relevant, the use of electronic identification means and trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust service for electronic transactions in the internal market, as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 as came into force on IP completion day as defined in the EU (Withdrawal Agreement) Act 2020, should be taken into account, in particular with regard to notified electronic identification schemes.

4. Dynamic linking is possible through the generation of authentication codes, which are subject to a set of strict security requirements. To remain technologically neutral, a specific technology for the implementation of authentication codes should not be required. Therefore authentication codes should be based on solutions such as generating and validating one-time passwords, digital signatures or other cryptographically underpinned validity assertions using keys or cryptographic material stored in the authentication elements, as long as the security requirements are fulfilled.

5. It is necessary to lay down specific requirements for the situation where the final amount is not known at the moment the payer initiates an electronic remote payment transaction, in order to ensure that the strong customer authentication is specific to the maximum amount that the payer has given consent for as referred to in the Payment Services Regulations 2017 (SI 2017/752).

6. In order to ensure the application of strong customer authentication, it is also necessary to require adequate security features for the elements of strong customer authentication categorised as knowledge (something only the user knows), such as length or complexity, for the elements categorised as possession (something only the user possesses), such as algorithm specifications, key length and information entropy, and for the devices and software that read elements categorised as inherence (something the user is), such as algorithm specifications, and biometric sensor and template protection features, in particular to mitigate the risk that those elements are uncovered, disclosed to and used by unauthorised parties. It is also necessary to lay down the requirements to ensure that those elements are independent, so that the breach of one does not compromise the reliability of the others, in particular when any of these elements are used through a multi-purpose device, such as a tablet or a mobile phone which can be used both for giving the instruction to make the payment and in the authentication process.

7. The requirements of strong customer authentication apply to payments initiated by the payer, regardless of whether the payer is a natural person or a legal entity.

8. Due to their very nature, payments made through the use of an anonymous payment instrument are not subject to the obligation of strong customer authentication. Where the anonymity of such instruments is lifted on contractual or legislative grounds, payments are subject to the security requirements that follow from the Payment Services Regulations 2017 (SI 2017/752) and this Regulatory Technical Standard.

9. In accordance with the Payment Services Regulations 2017 (SI 2017/752), exemptions to the principle of strong customer authentication have been defined based on the level of risk, amount, recurrence and the payment channel used for the execution of the payment transaction.

10. Actions which imply access to the balance and the recent transactions of a payment account without disclosure of sensitive payment data, recurring payments to the same payees which have been previously set up or confirmed by the payer through the use of strong customer authentication, and payments to and from the same natural or legal person with accounts with the same payment service provider pose a low level of risk, thus allowing payment service providers not to apply strong customer authentication. This leaves aside that in accordance with Regulations 68, 69 and 70 of the Payment Services Regulations 2017 (SI 2017/752), payment initiation service providers, payment service providers issuing card-based payment instruments and account information service providers should only seek and

obtain the necessary and essential information from the account servicing payment service provider for the provision of a given payment service with the consent of the payment service user. Such consent can be given individually for each request of information or for each payment to be initiated or, for account information service providers, as a mandate for designated payment accounts and associated payment transactions as established in the contractual agreement with the payment service user.

11. Exemptions for low-value contactless payments at points of sale, which also take into account a maximum number of consecutive transactions or a certain fixed maximum value of consecutive transactions without applying strong customer authentication, allow for the development of user-friendly and low-risk payment services and should therefore be provided for. It is also appropriate to establish an exemption for the case of electronic payment transactions initiated at unattended terminals, where the use of strong customer authentication may not always be easy to apply due to operational reasons (e.g. to avoid queues and potential accidents at toll gates or for other safety or security risks).

12. Similar to the exemption for low-value contactless payments at the point of sale, a proper balance needs to be struck between the interest in enhanced security in remote payments and the needs of user-friendliness and accessibility of payments in the area of e-commerce. In line with those principles, thresholds below which no strong customer authentication needs to be applied should be set in a prudent manner, to cover only online purchases of low value. The thresholds for online purchases should be set more prudently, considering that the fact that the person is not physically present when making the purchase poses a slightly higher security risk.

13. The requirements of strong customer authentication apply to payments initiated by the payer, regardless of whether the payer is a natural person or a legal entity. Many corporate payments are initiated through dedicated processes or protocols which guarantee the high levels of payment security that the Payment Services Regulations 2017 (SI 2017/752) aims to achieve through strong customer authentication. Where the FCA establishes that those payment processes and protocols that are only made available to payers who are not consumers achieve the objectives of the Payment Services Regulations 2017 (SI 2017/752) in terms of security, payment service providers may, in relation to those processes or protocols, be exempted from the strong customer authentication requirements.

14. In the case of real-time transaction risk analysis that categorises a payment transaction as low risk, it is also appropriate to introduce an exemption for the payment service provider that intends not to apply strong customer authentication through the adoption of effective and risk-based requirements which ensure the safety of the payment service user's funds and personal data. Those risk-based requirements should combine the scores of the risk analysis, confirming that no abnormal spending or behavioural pattern of the payer has been identified, taking into account other risk factors including information on the location of the payer and of the payee with monetary thresholds based on fraud rates calculated for remote payments. Where, on the basis of the real-time transaction risk analysis, a payment cannot be qualified as posing a low level of risk, the payment service provider should revert to strong customer authentication. The maximum value of such risk-based exemption should be set in a manner ensuring a very low corresponding fraud rate, also by comparison to the fraud rates of all the payment transactions of the payment service provider, including those authenticated through strong customer authentication, within a certain period of time and on a rolling basis.

15. For the purpose of ensuring an effective enforcement, payment service providers that wish to benefit from the exemptions from strong customer authentication should regularly monitor and make available to the FCA upon its request, for each payment transaction type, the value of fraudulent or unauthorised payment transactions and the observed fraud rates for all their payment transactions, whether authenticated through strong customer authentication or executed under a relevant exemption.

16. The collection of this new historical evidence on the fraud rates of electronic payment transactions will also contribute to an effective review by the FCA of the thresholds for an exemption to strong customer authentication based on a real-time transaction risk analysis. The FCA should review and, if appropriate, update these Standards, including where appropriate the thresholds and fraud rates, with the aim of enhancing the security of remote electronic payments, on a regular basis to take account of innovation and technical developments as well as other relevant matters.

17. Payment service providers that make use of any of the exemptions to be provided for should be allowed at any time to choose to apply strong customer authentication to the actions and to the payment transactions referred to in those provisions.
18. The measures that protect the confidentiality and integrity of personalised security credentials, as well as authentication devices and software, should limit the risks relating to fraud through unauthorised or fraudulent use of payment instruments and unauthorised access to payment accounts. To this end it is necessary to introduce requirements on the secure creation and delivery of the personalised security credentials and their association with the payment service user, and to provide conditions for the renewal and deactivation of those credentials.
19. In order to ensure effective and secure communication between the relevant actors in the context of account information services, payment initiation services and confirmation on the availability of funds, it is necessary to specify the requirements of common and secure open standards of communication to be met by all relevant payment service providers. The Payment Services Regulations 2017 (SI 2017/752) provide for the access and use of payment account information by account information service providers. These Standards therefore do not change the rules of access to accounts other than payment accounts.
20. Each account servicing payment service provider with payment accounts that are accessible online should offer at least one access interface enabling secure communication with account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. The interface should enable the account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments to identify themselves to the account servicing payment service provider. It should also allow account information service providers and payment initiation service providers to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user.
FCA 2021/45 To ensure technology and business model neutrality, the account servicing payment service providers should be free to decide whether to offer an interface that is dedicated to the communication with account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments, or to allow, for that communication, the use of the interface for the identification and communication with the account servicing payment service providers' payment service users.
21. In order to allow account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments to develop their technical solutions, the technical specification of the interface should be adequately documented and made publicly available. The effect of Articles 30(3) and (5) is that the account servicing payment service provider should offer a facility enabling the payment service providers to test the technical solutions
at least six months prior to by FCA 2021/45 the date on which the interface will be launched to the market. To ensure the interoperability of different technological communication solutions, the interface should use standards of communication which are developed by international standardisation organisations.
22. The quality of the services provided by account information service providers and payment initiation service providers will depend on the proper functioning of the interfaces put in place or adapted by account servicing payment service providers. It is therefore important that in case of non-compliance of such interfaces with the provisions included in these Standards, measures are taken to guarantee business continuity for the benefit of the users of those services. It is the responsibility of the FCA to ensure that account information service providers and payment initiation service providers are not blocked or obstructed in the provision of their services.
23. Where access to payment accounts is offered by means of a dedicated interface, in order to ensure the right of payment service users to make use of payment initiation service providers and of services enabling access to account information, as provided for in the Payment Services Regulations 2017 (SI 2017/752), it is necessary to require that dedicated interfaces have the same level of availability and performance as the interface available to the payment service user. Account servicing payment service providers should also define transparent key performance indicators and service level targets for the availability and performance of dedicated interfaces that are at least as stringent as those for the inter-

face used for their payment service users. Those interfaces should be tested by the payment service providers who will use them, and should be stress-tested and monitored by the FCA.

24. To ensure that payment service providers who rely on the dedicated interface can continue to provide their services in case of problems of availability or inadequate performance, it is necessary to provide, subject to strict conditions, a fallback mechanism that will allow such providers to use the interface that the account servicing payment service provider maintains for the identification of, and communication with, its own payment service users. Certain account servicing payment service providers will be exempted from having to provide such a fallback mechanism through their customer-facing interfaces where the FCA establishes that the dedicated interfaces comply with specific conditions that ensure unhampered competition. In the event that the exempted dedicated interfaces fail to comply with the required conditions, the granted exemptions shall be revoked by the FCA.

25. In order to allow the FCA to effectively supervise and monitor the implementation and management of the communication interfaces, the account servicing payment service providers should make a summary of the relevant documentation available on their website, and provide, upon request, the FCA with documentation of the solutions in case of emergencies. The account servicing payment service providers should also make publicly available the statistics on the availability and performance of that interface.

26. In order to safeguard the confidentiality and the integrity of data, it is necessary to ensure the security of communication sessions between account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. It is in particular necessary to require that secure encryption is applied between account information service providers, payment initiation service providers, payment service providers issuing card-based payment instruments and account servicing payment service providers when exchanging data.

27. To improve user confidence and ensure strong customer authentication, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall identify themselves to account servicing payment service providers using a form of identification issued by an independent third party. Where relevant, the use of electronic identification means and trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust service for electronic transactions in the internal market, as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 as came into force on IP completion day as defined in the EU (Withdrawal Agreement) Act 2020, should be taken into account, in particular with regard to notified electronic identification schemes.

5. It is necessary to lay down specific requirements for the situation where the final amount is not known at the moment the payer initiates an electronic remote payment transaction, in order to ensure that the strong customer authentication is specific to the maximum amount that the payer has given consent for as referred to in the Payment Services Regulations 2017 (SI 2017/752).

6. In order to ensure the application of strong customer authentication, it is also necessary to require adequate security features for the elements of strong customer authentication categorised as knowledge (something only the user knows), such as length or complexity, for the elements categorised as possession (something only the user possesses), such as algorithm specifications, key length and information entropy, and for the devices and software that read elements categorised as inherence (something the user is), such as algorithm specifications, and biometric sensor and template protection features, in particular to mitigate the risk that those elements are uncovered, disclosed to and used by unauthorised parties. It is also necessary to lay down the requirements to ensure that those elements are independent, so that the breach of one does not compromise the reliability of the others, in particular when any of these elements are used through a multi-purpose device, such as a tablet or a mobile phone which can be used both for giving the instruction to make the payment and in the authentication process.

7. The requirements of strong customer authentication apply to payments initiated by the payer, regardless of whether the payer is a natural person or a legal entity.

8. Due to their very nature, payments made through the use of an anonymous payment instrument are not subject to the obligation of strong customer authentication. Where the anonymity of such instruments is lifted on contractual or legislative grounds, payments are subject to the security requirements that follow from the Payment Services Regulations 2017 (SI 2017/752) and this Regulatory Technical Standard.

9. In accordance with the Payment Services Regulations 2017 (SI 2017/752), exemptions to the principle of strong customer authentication have been defined based on the level of risk, amount, recurrence and the payment channel used for the execution of the payment transaction.

10. Actions which imply access to the balance and the recent transactions of a payment account without disclosure of sensitive payment data, recurring payments to the same payees which have been previously set up or confirmed by the payer through the use of strong customer authentication, and payments to and from the same natural or legal person with accounts with the same payment service provider pose a low level of risk, thus allowing payment service providers not to apply strong customer authentication. This leaves aside that in accordance with Regulations 68, 69 and 70 of the Payment Services Regulations 2017 (SI 2017/752), payment initiation service providers, payment service providers issuing card-based payment instruments and account information service providers should only seek and obtain the necessary and essential information from the account servicing payment service provider for the provision of a given payment service with the consent of the payment service user. Such consent can be given individually for each request of information or for each payment to be initiated or, for account information service providers, as a mandate for designated payment accounts and associated payment transactions as established in the contractual agreement with the payment service user.

11. Exemptions for low-value contactless payments at points of sale, which also take into account a maximum number of consecutive transactions or a certain fixed maximum value of consecutive transactions without applying strong customer authentication, allow for the development of user-friendly and low-risk payment services and should therefore be provided for. It is also appropriate to establish an exemption for the case of electronic payment transactions initiated at unattended terminals, where the use of strong customer authentication may not always be easy to apply due to operational reasons (e.g. to avoid queues and potential accidents at toll gates or for other safety or security risks).

12. Similar to the exemption for low-value contactless payments at the point of sale, a proper balance needs to be struck between the interest in enhanced security in remote payments and the needs of user-friendliness and accessibility of payments in the area of e-commerce. In line with those principles, thresholds below which no strong customer authentication needs to be applied should be set in a prudent manner, to cover only online purchases of low value. The thresholds for online purchases should be set more prudently, considering that the fact that the person is not physically present when making the purchase poses a slightly higher security risk.

13. The requirements of strong customer authentication apply to payments initiated by the payer, regardless of whether the payer is a natural person or a legal entity. Many corporate payments are initiated through dedicated processes or protocols which guarantee the high levels of payment security that the Payment Services Regulations 2017 (SI 2017/752) aims to achieve through strong customer authentication. Where the FCA establishes that those payment processes and protocols that are only made available to payers who are not consumers achieve the objectives of the Payment Services Regulations 2017 (SI 2017/752) in terms of security, payment service providers may, in relation to those processes or protocols, be exempted from the strong customer authentication requirements.

14. In the case of real-time transaction risk analysis that categorises a payment transaction as low risk, it is also appropriate to introduce an exemption for the payment service provider that intends not to apply strong customer authentication through the adoption of effective and risk-based requirements which ensure the safety of the payment service user's funds and personal data. Those risk-based requirements should combine the scores of the risk analysis, confirming that no abnormal spending or behavioural pattern of the payer has been identified, taking into account other risk factors including information on the location of the payer and of the payee with monetary thresholds based on fraud rates calculated for remote payments. Where, on the basis of the real-time transaction risk analysis, a payment cannot be qualified as posing a low level of risk, the payment service provider should revert to strong customer authentication. The maximum value of such risk-based exemption should

be set in a manner ensuring a very low corresponding fraud rate, also by comparison to the fraud rates of all the payment transactions of the payment service provider, including those authenticated through strong customer authentication, within a certain period of time and on a rolling basis.

15. For the purpose of ensuring an effective enforcement, payment service providers that wish to benefit from the exemptions from strong customer authentication should regularly monitor and make available to the FCA upon its request, for each payment transaction type, the value of fraudulent or unauthorised payment transactions and the observed fraud rates for all their payment transactions, whether authenticated through strong customer authentication or executed under a relevant exemption.

16. The collection of this new historical evidence on the fraud rates of electronic payment transactions will also contribute to an effective review by the FCA of the thresholds for an exemption to strong customer authentication based on a real-time transaction risk analysis. The FCA should review and, if appropriate, update these Standards, including where appropriate the thresholds and fraud rates, with the aim of enhancing the security of remote electronic payments, on a regular basis to take account of innovation and technical developments as well as other relevant matters.

17. Payment service providers that make use of any of the exemptions to be provided for should be allowed at any time to choose to apply strong customer authentication to the actions and to the payment transactions referred to in those provisions.

18. The measures that protect the confidentiality and integrity of personalised security credentials, as well as authentication devices and software, should limit the risks relating to fraud through unauthorised or fraudulent use of payment instruments and unauthorised access to payment accounts. To this end it is necessary to introduce requirements on the secure creation and delivery of the personalised security credentials and their association with the payment service user, and to provide conditions for the renewal and deactivation of those credentials.

19. In order to ensure effective and secure communication between the relevant actors in the context of account information services, payment initiation services and confirmation on the availability of funds, it is necessary to specify the requirements of common and secure open standards of communication to be met by all relevant payment service providers. The Payment Services Regulations 2017 (SI 2017/752) provide for the access and use of payment account information by account information service providers. These Standards therefore do not change the rules of access to accounts other than payment accounts.

20. Each account servicing payment service provider with payment accounts that are accessible online should offer at least one access interface enabling secure communication with account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. The interface should enable the account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments to identify themselves to the account servicing payment service provider. It should also allow account information service providers and payment initiation service providers to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user.

FCA 2021/45 To ensure technology and business model neutrality, the account servicing payment service providers should be free to decide whether to offer an interface that is dedicated to the communication with account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments, or to allow, for that communication, the use of the interface for the identification and communication with the account servicing payment service providers' payment service users.

21. In order to allow account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments to develop their technical solutions, the technical specification of the interface should be adequately documented and made publicly available. The effect of Articles 30(3) and (5) is that the account servicing payment service provider should offer a facility enabling the payment service providers to test the technical solutions

at least six months prior to by FCA 2021/45 the date on which the interface will be launched to the market. To ensure the interoperability of different technological communic-

ation solutions, the interface should use standards of communication which are developed by international standardisation organisations.

22. The quality of the services provided by account information service providers and payment initiation service providers will depend on the proper functioning of the interfaces put in place or adapted by account servicing payment service providers. It is therefore important that in case of non-compliance of such interfaces with the provisions included in these Standards, measures are taken to guarantee business continuity for the benefit of the users of those services. It is the responsibility of the FCA to ensure that account information service providers and payment initiation service providers are not blocked or obstructed in the provision of their services.

23. Where access to payment accounts is offered by means of a dedicated interface, in order to ensure the right of payment service users to make use of payment initiation service providers and of services enabling access to account information, as provided for in the Payment Services Regulations 2017 (SI 2017/752), it is necessary to require that dedicated interfaces have the same level of availability and performance as the interface available to the payment service user. Account servicing payment service providers should also define transparent key performance indicators and service level targets for the availability and performance of dedicated interfaces that are at least as stringent as those for the interface used for their payment service users. Those interfaces should be tested by the payment service providers who will use them, and should be stress-tested and monitored by the FCA.

24. To ensure that payment service providers who rely on the dedicated interface can continue to provide their services in case of problems of availability or inadequate performance, it is necessary to provide, subject to strict conditions, a fallback mechanism that will allow such providers to use the interface that the account servicing payment service provider maintains for the identification of, and communication with, its own payment service users. Certain account servicing payment service providers will be exempted from having to provide such a fallback mechanism through their customer-facing interfaces where the FCA establishes that the dedicated interfaces comply with specific conditions that ensure unhampered competition. In the event that the exempted dedicated interfaces fail to comply with the required conditions, the granted exemptions shall be revoked by the FCA.

25. In order to allow the FCA to effectively supervise and monitor the implementation and management of the communication interfaces, the account servicing payment service providers should make a summary of the relevant documentation available on their website, and provide, upon request, the FCA with documentation of the solutions in case of emergencies. The account servicing payment service providers should also make publicly available the statistics on the availability and performance of that interface.

26. In order to safeguard the confidentiality and the integrity of data, it is necessary to ensure the security of communication sessions between account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. It is in particular necessary to require that secure encryption is applied between account information service providers, payment initiation service providers, payment service providers issuing card-based payment instruments and account servicing payment service providers when exchanging data.

27. To improve user confidence and ensure strong customer authentication, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall identify themselves to account servicing payment service providers using a form of identification issued by an independent third party. Where relevant, the use of electronic identification means and trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust service for electronic transactions in the internal market, as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 as came into force on IP completion day as defined in the EU (Withdrawal Agreement) Act 2020, should be taken into account, in particular with regard to notified electronic identification schemes.

6. In order to ensure the application of strong customer authentication, it is also necessary to require adequate security features for the elements of strong customer authentication categorised as knowledge (something only the user knows), such as length or

1

complexity, for the elements categorised as possession (something only the user possesses), such as algorithm specifications, key length and information entropy, and for the devices and software that read elements categorised as inherence (something the user is), such as algorithm specifications, and biometric sensor and template protection features, in particular to mitigate the risk that those elements are uncovered, disclosed to and used by unauthorised parties. It is also necessary to lay down the requirements to ensure that those elements are independent, so that the breach of one does not compromise the reliability of the others, in particular when any of these elements are used through a multi-purpose device, such as a tablet or a mobile phone which can be used both for giving the instruction to make the payment and in the authentication process.

7. The requirements of strong customer authentication apply to payments initiated by the payer, regardless of whether the payer is a natural person or a legal entity.

8. Due to their very nature, payments made through the use of an anonymous payment instrument are not subject to the obligation of strong customer authentication. Where the anonymity of such instruments is lifted on contractual or legislative grounds, payments are subject to the security requirements that follow from the Payment Services Regulations 2017 (SI 2017/752) and this Regulatory Technical Standard.

9. In accordance with the Payment Services Regulations 2017 (SI 2017/752), exemptions to the principle of strong customer authentication have been defined based on the level of risk, amount, recurrence and the payment channel used for the execution of the payment transaction.

10. Actions which imply access to the balance and the recent transactions of a payment account without disclosure of sensitive payment data, recurring payments to the same payees which have been previously set up or confirmed by the payer through the use of strong customer authentication, and payments to and from the same natural or legal person with accounts with the same payment service provider pose a low level of risk, thus allowing payment service providers not to apply strong customer authentication. This leaves aside that in accordance with Regulations 68, 69 and 70 of the Payment Services Regulations 2017 (SI 2017/752), payment initiation service providers, payment service providers issuing card-based payment instruments and account information service providers should only seek and obtain the necessary and essential information from the account servicing payment service provider for the provision of a given payment service with the consent of the payment service user. Such consent can be given individually for each request of information or for each payment to be initiated or, for account information service providers, as a mandate for designated payment accounts and associated payment transactions as established in the contractual agreement with the payment service user.

11. Exemptions for low-value contactless payments at points of sale, which also take into account a maximum number of consecutive transactions or a certain fixed maximum value of consecutive transactions without applying strong customer authentication, allow for the development of user-friendly and low-risk payment services and should therefore be provided for. It is also appropriate to establish an exemption for the case of electronic payment transactions initiated at unattended terminals, where the use of strong customer authentication may not always be easy to apply due to operational reasons (e.g. to avoid queues and potential accidents at toll gates or for other safety or security risks).

12. Similar to the exemption for low-value contactless payments at the point of sale, a proper balance needs to be struck between the interest in enhanced security in remote payments and the needs of user-friendliness and accessibility of payments in the area of e-commerce. In line with those principles, thresholds below which no strong customer authentication needs to be applied should be set in a prudent manner, to cover only online purchases of low value. The thresholds for online purchases should be set more prudently, considering that the fact that the person is not physically present when making the purchase poses a slightly higher security risk.

13. The requirements of strong customer authentication apply to payments initiated by the payer, regardless of whether the payer is a natural person or a legal entity. Many corporate payments are initiated through dedicated processes or protocols which guarantee the high levels of payment security that the Payment Services Regulations 2017 (SI 2017/752) aims to achieve through strong customer authentication. Where the FCA establishes that those payment processes and protocols that are only made available to payers who are not consumers achieve the objectives of the Payment Services Regulations 2017 (SI 2017/752)

in terms of security, payment service providers may, in relation to those processes or protocols, be exempted from the strong customer authentication requirements.

14. In the case of real-time transaction risk analysis that categorises a payment transaction as low risk, it is also appropriate to introduce an exemption for the payment service provider that intends not to apply strong customer authentication through the adoption of effective and risk-based requirements which ensure the safety of the payment service user's funds and personal data. Those risk-based requirements should combine the scores of the risk analysis, confirming that no abnormal spending or behavioural pattern of the payer has been identified, taking into account other risk factors including information on the location of the payer and of the payee with monetary thresholds based on fraud rates calculated for remote payments. Where, on the basis of the real-time transaction risk analysis, a payment cannot be qualified as posing a low level of risk, the payment service provider should revert to strong customer authentication. The maximum value of such risk-based exemption should be set in a manner ensuring a very low corresponding fraud rate, also by comparison to the fraud rates of all the payment transactions of the payment service provider, including those authenticated through strong customer authentication, within a certain period of time and on a rolling basis.

15. For the purpose of ensuring an effective enforcement, payment service providers that wish to benefit from the exemptions from strong customer authentication should regularly monitor and make available to the FCA upon its request, for each payment transaction type, the value of fraudulent or unauthorised payment transactions and the observed fraud rates for all their payment transactions, whether authenticated through strong customer authentication or executed under a relevant exemption.

16. The collection of this new historical evidence on the fraud rates of electronic payment transactions will also contribute to an effective review by the FCA of the thresholds for an exemption to strong customer authentication based on a real-time transaction risk analysis. The FCA should review and, if appropriate, update these Standards, including where appropriate the thresholds and fraud rates, with the aim of enhancing the security of remote electronic payments, on a regular basis to take account of innovation and technical developments as well as other relevant matters.

17. Payment service providers that make use of any of the exemptions to be provided for should be allowed at any time to choose to apply strong customer authentication to the actions and to the payment transactions referred to in those provisions.

18. The measures that protect the confidentiality and integrity of personalised security credentials, as well as authentication devices and software, should limit the risks relating to fraud through unauthorised or fraudulent use of payment instruments and unauthorised access to payment accounts. To this end it is necessary to introduce requirements on the secure creation and delivery of the personalised security credentials and their association with the payment service user, and to provide conditions for the renewal and deactivation of those credentials.

19. In order to ensure effective and secure communication between the relevant actors in the context of account information services, payment initiation services and confirmation on the availability of funds, it is necessary to specify the requirements of common and secure open standards of communication to be met by all relevant payment service providers. The Payment Services Regulations 2017 (SI 2017/752) provide for the access and use of payment account information by account information service providers. These Standards therefore do not change the rules of access to accounts other than payment accounts.

20. Each account servicing payment service provider with payment accounts that are accessible online should offer at least one access interface enabling secure communication with account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. The interface should enable the account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments to identify themselves to the account servicing payment service provider. It should also allow account information service providers and payment initiation service providers to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user.

FCA 2021/45 To ensure technology and business model neutrality, the account servicing payment service providers should be free to decide whether to offer an interface that is dedicated to the communication with account information service providers, payment initi-

ation service providers, and payment service providers issuing card-based payment instruments, or to allow, for that communication, the use of the interface for the identification and communication with the account servicing payment service providers' payment service users.

21. In order to allow account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments to develop their technical solutions, the technical specification of the interface should be adequately documented and made publicly available. The effect of Articles 30(3) and (5) is that the account servicing payment service provider should offer a facility enabling the payment service providers to test the technical solutions

at least six months prior to by FCA 2021/45 the date on which the interface will be launched to the market. To ensure the interoperability of different technological communication solutions, the interface should use standards of communication which are developed by international standardisation organisations.

22. The quality of the services provided by account information service providers and payment initiation service providers will depend on the proper functioning of the interfaces put in place or adapted by account servicing payment service providers. It is therefore important that in case of non-compliance of such interfaces with the provisions included in these Standards, measures are taken to guarantee business continuity for the benefit of the users of those services. It is the responsibility of the FCA to ensure that account information service providers and payment initiation service providers are not blocked or obstructed in the provision of their services.

23. Where access to payment accounts is offered by means of a dedicated interface, in order to ensure the right of payment service users to make use of payment initiation service providers and of services enabling access to account information, as provided for in the Payment Services Regulations 2017 (SI 2017/752), it is necessary to require that dedicated interfaces have the same level of availability and performance as the interface available to the payment service user. Account servicing payment service providers should also define transparent key performance indicators and service level targets for the availability and performance of dedicated interfaces that are at least as stringent as those for the interface used for their payment service users. Those interfaces should be tested by the payment service providers who will use them, and should be stress-tested and monitored by the FCA.

24. To ensure that payment service providers who rely on the dedicated interface can continue to provide their services in case of problems of availability or inadequate performance, it is necessary to provide, subject to strict conditions, a fallback mechanism that will allow such providers to use the interface that the account servicing payment service provider maintains for the identification of, and communication with, its own payment service users. Certain account servicing payment service providers will be exempted from having to provide such a fallback mechanism through their customer-facing interfaces where the FCA establishes that the dedicated interfaces comply with specific conditions that ensure unhampered competition. In the event that the exempted dedicated interfaces fail to comply with the required conditions, the granted exemptions shall be revoked by the FCA.

25. In order to allow the FCA to effectively supervise and monitor the implementation and management of the communication interfaces, the account servicing payment service providers should make a summary of the relevant documentation available on their website, and provide, upon request, the FCA with documentation of the solutions in case of emergencies. The account servicing payment service providers should also make publicly available the statistics on the availability and performance of that interface.

26. In order to safeguard the confidentiality and the integrity of data, it is necessary to ensure the security of communication sessions between account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. It is in particular necessary to require that secure encryption is applied between account information service providers, payment initiation service providers, payment service providers issuing card-based payment instruments and account servicing payment service providers when exchanging data.

27. To improve user confidence and ensure strong customer authentication, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall identify themselves to account servicing payment service providers using a form of identification issued by an independent third

party. Where relevant, the use of electronic identification means and trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust service for electronic transactions in the internal market, as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 as came into force on IP completion day as defined in the EU (Withdrawal Agreement) Act 2020, should be taken into account, in particular with regard to notified electronic identification schemes.

7. The requirements of strong customer authentication apply to payments initiated by the payer, regardless of whether the payer is a natural person or a legal entity.
8. Due to their very nature, payments made through the use of an anonymous payment instrument are not subject to the obligation of strong customer authentication. Where the anonymity of such instruments is lifted on contractual or legislative grounds, payments are subject to the security requirements that follow from the Payment Services Regulations 2017 (SI 2017/752) and this Regulatory Technical Standard.
9. In accordance with the Payment Services Regulations 2017 (SI 2017/752), exemptions to the principle of strong customer authentication have been defined based on the level of risk, amount, recurrence and the payment channel used for the execution of the payment transaction.
10. Actions which imply access to the balance and the recent transactions of a payment account without disclosure of sensitive payment data, recurring payments to the same payees which have been previously set up or confirmed by the payer through the use of strong customer authentication, and payments to and from the same natural or legal person with accounts with the same payment service provider pose a low level of risk, thus allowing payment service providers not to apply strong customer authentication. This leaves aside that in accordance with Regulations 68, 69 and 70 of the Payment Services Regulations 2017 (SI 2017/752), payment initiation service providers, payment service providers issuing card-based payment instruments and account information service providers should only seek and obtain the necessary and essential information from the account servicing payment service provider for the provision of a given payment service with the consent of the payment service user. Such consent can be given individually for each request of information or for each payment to be initiated or, for account information service providers, as a mandate for designated payment accounts and associated payment transactions as established in the contractual agreement with the payment service user.
11. Exemptions for low-value contactless payments at points of sale, which also take into account a maximum number of consecutive transactions or a certain fixed maximum value of consecutive transactions without applying strong customer authentication, allow for the development of user-friendly and low-risk payment services and should therefore be provided for. It is also appropriate to establish an exemption for the case of electronic payment transactions initiated at unattended terminals, where the use of strong customer authentication may not always be easy to apply due to operational reasons (e.g. to avoid queues and potential accidents at toll gates or for other safety or security risks).
12. Similar to the exemption for low-value contactless payments at the point of sale, a proper balance needs to be struck between the interest in enhanced security in remote payments and the needs of user-friendliness and accessibility of payments in the area of e-commerce. In line with those principles, thresholds below which no strong customer authentication needs to be applied should be set in a prudent manner, to cover only online purchases of low value. The thresholds for online purchases should be set more prudently, considering that the fact that the person is not physically present when making the purchase poses a slightly higher security risk.
13. The requirements of strong customer authentication apply to payments initiated by the payer, regardless of whether the payer is a natural person or a legal entity. Many corporate payments are initiated through dedicated processes or protocols which guarantee the high levels of payment security that the Payment Services Regulations 2017 (SI 2017/752) aims to achieve through strong customer authentication. Where the FCA establishes that those payment processes and protocols that are only made available to payers who are not consumers achieve the objectives of the Payment Services Regulations 2017 (SI 2017/752) in terms of security, payment service providers may, in relation to those processes or protocols, be exempted from the strong customer authentication requirements.

14. In the case of real-time transaction risk analysis that categorises a payment transaction as low risk, it is also appropriate to introduce an exemption for the payment service provider that intends not to apply strong customer authentication through the adoption of effective and risk-based requirements which ensure the safety of the payment service user's funds and personal data. Those risk-based requirements should combine the scores of the risk analysis, confirming that no abnormal spending or behavioural pattern of the payer has been identified, taking into account other risk factors including information on the location of the payer and of the payee with monetary thresholds based on fraud rates calculated for remote payments. Where, on the basis of the real-time transaction risk analysis, a payment cannot be qualified as posing a low level of risk, the payment service provider should revert to strong customer authentication. The maximum value of such risk-based exemption should be set in a manner ensuring a very low corresponding fraud rate, also by comparison to the fraud rates of all the payment transactions of the payment service provider, including those authenticated through strong customer authentication, within a certain period of time and on a rolling basis.

15. For the purpose of ensuring an effective enforcement, payment service providers that wish to benefit from the exemptions from strong customer authentication should regularly monitor and make available to the FCA upon its request, for each payment transaction type, the value of fraudulent or unauthorised payment transactions and the observed fraud rates for all their payment transactions, whether authenticated through strong customer authentication or executed under a relevant exemption.

16. The collection of this new historical evidence on the fraud rates of electronic payment transactions will also contribute to an effective review by the FCA of the thresholds for an exemption to strong customer authentication based on a real-time transaction risk analysis. The FCA should review and, if appropriate, update these Standards, including where appropriate the thresholds and fraud rates, with the aim of enhancing the security of remote electronic payments, on a regular basis to take account of innovation and technical developments as well as other relevant matters.

17. Payment service providers that make use of any of the exemptions to be provided for should be allowed at any time to choose to apply strong customer authentication to the actions and to the payment transactions referred to in those provisions.

18. The measures that protect the confidentiality and integrity of personalised security credentials, as well as authentication devices and software, should limit the risks relating to fraud through unauthorised or fraudulent use of payment instruments and unauthorised access to payment accounts. To this end it is necessary to introduce requirements on the secure creation and delivery of the personalised security credentials and their association with the payment service user, and to provide conditions for the renewal and deactivation of those credentials.

19. In order to ensure effective and secure communication between the relevant actors in the context of account information services, payment initiation services and confirmation on the availability of funds, it is necessary to specify the requirements of common and secure open standards of communication to be met by all relevant payment service providers. The Payment Services Regulations 2017 (SI 2017/752) provide for the access and use of payment account information by account information service providers. These Standards therefore do not change the rules of access to accounts other than payment accounts.

20. Each account servicing payment service provider with payment accounts that are accessible online should offer at least one access interface enabling secure communication with account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. The interface should enable the account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments to identify themselves to the account servicing payment service provider. It should also allow account information service providers and payment initiation service providers to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user.

FCA 2021/45 To ensure technology and business model neutrality, the account servicing payment service providers should be free to decide whether to offer an interface that is dedicated to the communication with account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments, or to allow, for that communication, the use of the interface for the identification

and communication with the account servicing payment service providers' payment service users.

21. In order to allow account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments to develop their technical solutions, the technical specification of the interface should be adequately documented and made publicly available. The effect of Articles 30(3) and (5) is that the account servicing payment service provider should offer a facility enabling the payment service providers to test the technical solutions

at least six months prior to by FCA 2021/45 the date on which the interface will be launched to the market. To ensure the interoperability of different technological communication solutions, the interface should use standards of communication which are developed by international standardisation organisations.

22. The quality of the services provided by account information service providers and payment initiation service providers will depend on the proper functioning of the interfaces put in place or adapted by account servicing payment service providers. It is therefore important that in case of non-compliance of such interfaces with the provisions included in these Standards, measures are taken to guarantee business continuity for the benefit of the users of those services. It is the responsibility of the FCA to ensure that account information service providers and payment initiation service providers are not blocked or obstructed in the provision of their services.

23. Where access to payment accounts is offered by means of a dedicated interface, in order to ensure the right of payment service users to make use of payment initiation service providers and of services enabling access to account information, as provided for in the Payment Services Regulations 2017 (SI 2017/752), it is necessary to require that dedicated interfaces have the same level of availability and performance as the interface available to the payment service user. Account servicing payment service providers should also define transparent key performance indicators and service level targets for the availability and performance of dedicated interfaces that are at least as stringent as those for the interface used for their payment service users. Those interfaces should be tested by the payment service providers who will use them, and should be stress-tested and monitored by the FCA.

24. To ensure that payment service providers who rely on the dedicated interface can continue to provide their services in case of problems of availability or inadequate performance, it is necessary to provide, subject to strict conditions, a fallback mechanism that will allow such providers to use the interface that the account servicing payment service provider maintains for the identification of, and communication with, its own payment service users. Certain account servicing payment service providers will be exempted from having to provide such a fallback mechanism through their customer-facing interfaces where the FCA establishes that the dedicated interfaces comply with specific conditions that ensure unhampered competition. In the event that the exempted dedicated interfaces fail to comply with the required conditions, the granted exemptions shall be revoked by the FCA.

25. In order to allow the FCA to effectively supervise and monitor the implementation and management of the communication interfaces, the account servicing payment service providers should make a summary of the relevant documentation available on their website, and provide, upon request, the FCA with documentation of the solutions in case of emergencies. The account servicing payment service providers should also make publicly available the statistics on the availability and performance of that interface.

26. In order to safeguard the confidentiality and the integrity of data, it is necessary to ensure the security of communication sessions between account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. It is in particular necessary to require that secure encryption is applied between account information service providers, payment initiation service providers, payment service providers issuing card-based payment instruments and account servicing payment service providers when exchanging data.

27. To improve user confidence and ensure strong customer authentication, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall identify themselves to account servicing payment service providers using a form of identification issued by an independent third party. Where relevant, the use of electronic identification means and trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July

1

2014 on electronic identification and trust service for electronic transactions in the internal market, as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 as came into force on IP completion day as defined in the EU (Withdrawal Agreement) Act 2020, should be taken into account, in particular with regard to notified electronic identification schemes.

8. Due to their very nature, payments made through the use of an anonymous payment instrument are not subject to the obligation of strong customer authentication. Where the anonymity of such instruments is lifted on contractual or legislative grounds, payments are subject to the security requirements that follow from the Payment Services Regulations 2017 (SI 2017/752) and this Regulatory Technical Standard.

9. In accordance with the Payment Services Regulations 2017 (SI 2017/752), exemptions to the principle of strong customer authentication have been defined based on the level of risk, amount, recurrence and the payment channel used for the execution of the payment transaction.

10. Actions which imply access to the balance and the recent transactions of a payment account without disclosure of sensitive payment data, recurring payments to the same payees which have been previously set up or confirmed by the payer through the use of strong customer authentication, and payments to and from the same natural or legal person with accounts with the same payment service provider pose a low level of risk, thus allowing payment service providers not to apply strong customer authentication. This leaves aside that in accordance with Regulations 68, 69 and 70 of the Payment Services Regulations 2017 (SI 2017/752), payment initiation service providers, payment service providers issuing card-based payment instruments and account information service providers should only seek and obtain the necessary and essential information from the account servicing payment service provider for the provision of a given payment service with the consent of the payment service user. Such consent can be given individually for each request of information or for each payment to be initiated or, for account information service providers, as a mandate for designated payment accounts and associated payment transactions as established in the contractual agreement with the payment service user.

11. Exemptions for low-value contactless payments at points of sale, which also take into account a maximum number of consecutive transactions or a certain fixed maximum value of consecutive transactions without applying strong customer authentication, allow for the development of user-friendly and low-risk payment services and should therefore be provided for. It is also appropriate to establish an exemption for the case of electronic payment transactions initiated at unattended terminals, where the use of strong customer authentication may not always be easy to apply due to operational reasons (e.g. to avoid queues and potential accidents at toll gates or for other safety or security risks).

12. Similar to the exemption for low-value contactless payments at the point of sale, a proper balance needs to be struck between the interest in enhanced security in remote payments and the needs of user-friendliness and accessibility of payments in the area of e-commerce. In line with those principles, thresholds below which no strong customer authentication needs to be applied should be set in a prudent manner, to cover only online purchases of low value. The thresholds for online purchases should be set more prudently, considering that the fact that the person is not physically present when making the purchase poses a slightly higher security risk.

13. The requirements of strong customer authentication apply to payments initiated by the payer, regardless of whether the payer is a natural person or a legal entity. Many corporate payments are initiated through dedicated processes or protocols which guarantee the high levels of payment security that the Payment Services Regulations 2017 (SI 2017/752) aims to achieve through strong customer authentication. Where the FCA establishes that those payment processes and protocols that are only made available to payers who are not consumers achieve the objectives of the Payment Services Regulations 2017 (SI 2017/752) in terms of security, payment service providers may, in relation to those processes or protocols, be exempted from the strong customer authentication requirements.

14. In the case of real-time transaction risk analysis that categorises a payment transaction as low risk, it is also appropriate to introduce an exemption for the payment service provider that intends not to apply strong customer authentication through the adoption of effective and risk-based requirements which ensure the safety of the payment service user's funds

and personal data. Those risk-based requirements should combine the scores of the risk analysis, confirming that no abnormal spending or behavioural pattern of the payer has been identified, taking into account other risk factors including information on the location of the payer and of the payee with monetary thresholds based on fraud rates calculated for remote payments. Where, on the basis of the real-time transaction risk analysis, a payment cannot be qualified as posing a low level of risk, the payment service provider should revert to strong customer authentication. The maximum value of such risk-based exemption should be set in a manner ensuring a very low corresponding fraud rate, also by comparison to the fraud rates of all the payment transactions of the payment service provider, including those authenticated through strong customer authentication, within a certain period of time and on a rolling basis.

15. For the purpose of ensuring an effective enforcement, payment service providers that wish to benefit from the exemptions from strong customer authentication should regularly monitor and make available to the FCA upon its request, for each payment transaction type, the value of fraudulent or unauthorised payment transactions and the observed fraud rates for all their payment transactions, whether authenticated through strong customer authentication or executed under a relevant exemption.

16. The collection of this new historical evidence on the fraud rates of electronic payment transactions will also contribute to an effective review by the FCA of the thresholds for an exemption to strong customer authentication based on a real-time transaction risk analysis. The FCA should review and, if appropriate, update these Standards, including where appropriate the thresholds and fraud rates, with the aim of enhancing the security of remote electronic payments, on a regular basis to take account of innovation and technical developments as well as other relevant matters.

17. Payment service providers that make use of any of the exemptions to be provided for should be allowed at any time to choose to apply strong customer authentication to the actions and to the payment transactions referred to in those provisions.

18. The measures that protect the confidentiality and integrity of personalised security credentials, as well as authentication devices and software, should limit the risks relating to fraud through unauthorised or fraudulent use of payment instruments and unauthorised access to payment accounts. To this end it is necessary to introduce requirements on the secure creation and delivery of the personalised security credentials and their association with the payment service user, and to provide conditions for the renewal and deactivation of those credentials.

19. In order to ensure effective and secure communication between the relevant actors in the context of account information services, payment initiation services and confirmation on the availability of funds, it is necessary to specify the requirements of common and secure open standards of communication to be met by all relevant payment service providers. The Payment Services Regulations 2017 (SI 2017/752) provide for the access and use of payment account information by account information service providers. These Standards therefore do not change the rules of access to accounts other than payment accounts.

20. Each account servicing payment service provider with payment accounts that are accessible online should offer at least one access interface enabling secure communication with account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. The interface should enable the account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments to identify themselves to the account servicing payment service provider. It should also allow account information service providers and payment initiation service providers to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user.

FCA 2021/45 To ensure technology and business model neutrality, the account servicing payment service providers should be free to decide whether to offer an interface that is dedicated to the communication with account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments, or to allow, for that communication, the use of the interface for the identification and communication with the account servicing payment service providers' payment service users.

21. In order to allow account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments to

1

develop their technical solutions, the technical specification of the interface should be adequately documented and made publicly available. The effect of Articles 30(3) and (5) is that the account servicing payment service provider should offer a facility enabling the payment service providers to test the technical solutions
at least six months prior to by FCA 2021/45 the date on which the interface will be launched to the market. To ensure the interoperability of different technological communication solutions, the interface should use standards of communication which are developed by international standardisation organisations.

22. The quality of the services provided by account information service providers and payment initiation service providers will depend on the proper functioning of the interfaces put in place or adapted by account servicing payment service providers. It is therefore important that in case of non-compliance of such interfaces with the provisions included in these Standards, measures are taken to guarantee business continuity for the benefit of the users of those services. It is the responsibility of the FCA to ensure that account information service providers and payment initiation service providers are not blocked or obstructed in the provision of their services.

23. Where access to payment accounts is offered by means of a dedicated interface, in order to ensure the right of payment service users to make use of payment initiation service providers and of services enabling access to account information, as provided for in the Payment Services Regulations 2017 (SI 2017/752), it is necessary to require that dedicated interfaces have the same level of availability and performance as the interface available to the payment service user. Account servicing payment service providers should also define transparent key performance indicators and service level targets for the availability and performance of dedicated interfaces that are at least as stringent as those for the interface used for their payment service users. Those interfaces should be tested by the payment service providers who will use them, and should be stress-tested and monitored by the FCA.

24. To ensure that payment service providers who rely on the dedicated interface can continue to provide their services in case of problems of availability or inadequate performance, it is necessary to provide, subject to strict conditions, a fallback mechanism that will allow such providers to use the interface that the account servicing payment service provider maintains for the identification of, and communication with, its own payment service users. Certain account servicing payment service providers will be exempted from having to provide such a fallback mechanism through their customer-facing interfaces where the FCA establishes that the dedicated interfaces comply with specific conditions that ensure unhampered competition. In the event that the exempted dedicated interfaces fail to comply with the required conditions, the granted exemptions shall be revoked by the FCA.

25. In order to allow the FCA to effectively supervise and monitor the implementation and management of the communication interfaces, the account servicing payment service providers should make a summary of the relevant documentation available on their website, and provide, upon request, the FCA with documentation of the solutions in case of emergencies. The account servicing payment service providers should also make publicly available the statistics on the availability and performance of that interface.

26. In order to safeguard the confidentiality and the integrity of data, it is necessary to ensure the security of communication sessions between account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. It is in particular necessary to require that secure encryption is applied between account information service providers, payment initiation service providers, payment service providers issuing card-based payment instruments and account servicing payment service providers when exchanging data.

27. To improve user confidence and ensure strong customer authentication, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall identify themselves to account servicing payment service providers using a form of identification issued by an independent third party. Where relevant, the use of electronic identification means and trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust service for electronic transactions in the internal market, as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 as came into force on IP completion

day as defined in the EU (Withdrawal Agreement) Act 2020, should be taken into account, in particular with regard to notified electronic identification schemes.

9. In accordance with the Payment Services Regulations 2017 (SI 2017/752), exemptions to the principle of strong customer authentication have been defined based on the level of risk, amount, recurrence and the payment channel used for the execution of the payment transaction.

10. Actions which imply access to the balance and the recent transactions of a payment account without disclosure of sensitive payment data, recurring payments to the same payees which have been previously set up or confirmed by the payer through the use of strong customer authentication, and payments to and from the same natural or legal person with accounts with the same payment service provider pose a low level of risk, thus allowing payment service providers not to apply strong customer authentication. This leaves aside that in accordance with Regulations 68, 69 and 70 of the Payment Services Regulations 2017 (SI 2017/752), payment initiation service providers, payment service providers issuing card-based payment instruments and account information service providers should only seek and obtain the necessary and essential information from the account servicing payment service provider for the provision of a given payment service with the consent of the payment service user. Such consent can be given individually for each request of information or for each payment to be initiated or, for account information service providers, as a mandate for designated payment accounts and associated payment transactions as established in the contractual agreement with the payment service user.

11. Exemptions for low-value contactless payments at points of sale, which also take into account a maximum number of consecutive transactions or a certain fixed maximum value of consecutive transactions without applying strong customer authentication, allow for the development of user-friendly and low-risk payment services and should therefore be provided for. It is also appropriate to establish an exemption for the case of electronic payment transactions initiated at unattended terminals, where the use of strong customer authentication may not always be easy to apply due to operational reasons (e.g. to avoid queues and potential accidents at toll gates or for other safety or security risks).

12. Similar to the exemption for low-value contactless payments at the point of sale, a proper balance needs to be struck between the interest in enhanced security in remote payments and the needs of user-friendliness and accessibility of payments in the area of e-commerce. In line with those principles, thresholds below which no strong customer authentication needs to be applied should be set in a prudent manner, to cover only online purchases of low value. The thresholds for online purchases should be set more prudently, considering that the fact that the person is not physically present when making the purchase poses a slightly higher security risk.

13. The requirements of strong customer authentication apply to payments initiated by the payer, regardless of whether the payer is a natural person or a legal entity. Many corporate payments are initiated through dedicated processes or protocols which guarantee the high levels of payment security that the Payment Services Regulations 2017 (SI 2017/752) aims to achieve through strong customer authentication. Where the FCA establishes that those payment processes and protocols that are only made available to payers who are not consumers achieve the objectives of the Payment Services Regulations 2017 (SI 2017/752) in terms of security, payment service providers may, in relation to those processes or protocols, be exempted from the strong customer authentication requirements.

14. In the case of real-time transaction risk analysis that categorises a payment transaction as low risk, it is also appropriate to introduce an exemption for the payment service provider that intends not to apply strong customer authentication through the adoption of effective and risk-based requirements which ensure the safety of the payment service user's funds and personal data. Those risk-based requirements should combine the scores of the risk analysis, confirming that no abnormal spending or behavioural pattern of the payer has been identified, taking into account other risk factors including information on the location of the payer and of the payee with monetary thresholds based on fraud rates calculated for remote payments. Where, on the basis of the real-time transaction risk analysis, a payment cannot be qualified as posing a low level of risk, the payment service provider should revert to strong customer authentication. The maximum value of such risk-based exemption should be set in a manner ensuring a very low corresponding fraud rate, also by comparison to the

1

fraud rates of all the payment transactions of the payment service provider, including those authenticated through strong customer authentication, within a certain period of time and on a rolling basis.

15. For the purpose of ensuring an effective enforcement, payment service providers that wish to benefit from the exemptions from strong customer authentication should regularly monitor and make available to the FCA upon its request, for each payment transaction type, the value of fraudulent or unauthorised payment transactions and the observed fraud rates for all their payment transactions, whether authenticated through strong customer authentication or executed under a relevant exemption.

16. The collection of this new historical evidence on the fraud rates of electronic payment transactions will also contribute to an effective review by the FCA of the thresholds for an exemption to strong customer authentication based on a real-time transaction risk analysis. The FCA should review and, if appropriate, update these Standards, including where appropriate the thresholds and fraud rates, with the aim of enhancing the security of remote electronic payments, on a regular basis to take account of innovation and technical developments as well as other relevant matters.

17. Payment service providers that make use of any of the exemptions to be provided for should be allowed at any time to choose to apply strong customer authentication to the actions and to the payment transactions referred to in those provisions.

18. The measures that protect the confidentiality and integrity of personalised security credentials, as well as authentication devices and software, should limit the risks relating to fraud through unauthorised or fraudulent use of payment instruments and unauthorised access to payment accounts. To this end it is necessary to introduce requirements on the secure creation and delivery of the personalised security credentials and their association with the payment service user, and to provide conditions for the renewal and deactivation of those credentials.

19. In order to ensure effective and secure communication between the relevant actors in the context of account information services, payment initiation services and confirmation on the availability of funds, it is necessary to specify the requirements of common and secure open standards of communication to be met by all relevant payment service providers. The Payment Services Regulations 2017 (SI 2017/752) provide for the access and use of payment account information by account information service providers. These Standards therefore do not change the rules of access to accounts other than payment accounts.

20. Each account servicing payment service provider with payment accounts that are accessible online should offer at least one access interface enabling secure communication with account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. The interface should enable the account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments to identify themselves to the account servicing payment service provider. It should also allow account information service providers and payment initiation service providers to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user.

FCA 2021/45 To ensure technology and business model neutrality, the account servicing payment service providers should be free to decide whether to offer an interface that is dedicated to the communication with account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments, or to allow, for that communication, the use of the interface for the identification and communication with the account servicing payment service providers' payment service users.

21. In order to allow account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments to develop their technical solutions, the technical specification of the interface should be adequately documented and made publicly available. The effect of Articles 30(3) and (5) is that the account servicing payment service provider should offer a facility enabling the payment service providers to test the technical solutions

at least six months prior to by FCA 2021/45 the date on which the interface will be launched to the market. To ensure the interoperability of different technological communication solutions, the interface should use standards of communication which are developed by international standardisation organisations.

22. The quality of the services provided by account information service providers and payment initiation service providers will depend on the proper functioning of the interfaces put in place or adapted by account servicing payment service providers. It is therefore important that in case of non-compliance of such interfaces with the provisions included in these Standards, measures are taken to guarantee business continuity for the benefit of the users of those services. It is the responsibility of the FCA to ensure that account information service providers and payment initiation service providers are not blocked or obstructed in the provision of their services.
23. Where access to payment accounts is offered by means of a dedicated interface, in order to ensure the right of payment service users to make use of payment initiation service providers and of services enabling access to account information, as provided for in the Payment Services Regulations 2017 (SI 2017/752), it is necessary to require that dedicated interfaces have the same level of availability and performance as the interface available to the payment service user. Account servicing payment service providers should also define transparent key performance indicators and service level targets for the availability and performance of dedicated interfaces that are at least as stringent as those for the interface used for their payment service users. Those interfaces should be tested by the payment service providers who will use them, and should be stress-tested and monitored by the FCA.
24. To ensure that payment service providers who rely on the dedicated interface can continue to provide their services in case of problems of availability or inadequate performance, it is necessary to provide, subject to strict conditions, a fallback mechanism that will allow such providers to use the interface that the account servicing payment service provider maintains for the identification of, and communication with, its own payment service users. Certain account servicing payment service providers will be exempted from having to provide such a fallback mechanism through their customer-facing interfaces where the FCA establishes that the dedicated interfaces comply with specific conditions that ensure unhampered competition. In the event that the exempted dedicated interfaces fail to comply with the required conditions, the granted exemptions shall be revoked by the FCA.
25. In order to allow the FCA to effectively supervise and monitor the implementation and management of the communication interfaces, the account servicing payment service providers should make a summary of the relevant documentation available on their website, and provide, upon request, the FCA with documentation of the solutions in case of emergencies. The account servicing payment service providers should also make publicly available the statistics on the availability and performance of that interface.
26. In order to safeguard the confidentiality and the integrity of data, it is necessary to ensure the security of communication sessions between account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. It is in particular necessary to require that secure encryption is applied between account information service providers, payment initiation service providers, payment service providers issuing card-based payment instruments and account servicing payment service providers when exchanging data.
27. To improve user confidence and ensure strong customer authentication, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall identify themselves to account servicing payment service providers using a form of identification issued by an independent third party. Where relevant, the use of electronic identification means and trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust service for electronic transactions in the internal market, as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 as came into force on IP completion day as defined in the EU (Withdrawal Agreement) Act 2020, should be taken into account, in particular with regard to notified electronic identification schemes.

10. Actions which imply access to the balance and the recent transactions of a payment account without disclosure of sensitive payment data, recurring payments to the same payees which have been previously set up or confirmed by the payer through the use of strong customer authentication, and payments to and from the same natural or legal person with accounts with the same payment service provider pose a low level of risk, thus allowing

1

payment service providers not to apply strong customer authentication. This leaves aside that in accordance with Regulations 68, 69 and 70 of the Payment Services Regulations 2017 (SI 2017/752), payment initiation service providers, payment service providers issuing card-based payment instruments and account information service providers should only seek and obtain the necessary and essential information from the account servicing payment service provider for the provision of a given payment service with the consent of the payment service user. Such consent can be given individually for each request of information or for each payment to be initiated or, for account information service providers, as a mandate for designated payment accounts and associated payment transactions as established in the contractual agreement with the payment service user.

11. Exemptions for low-value contactless payments at points of sale, which also take into account a maximum number of consecutive transactions or a certain fixed maximum value of consecutive transactions without applying strong customer authentication, allow for the development of user-friendly and low-risk payment services and should therefore be provided for. It is also appropriate to establish an exemption for the case of electronic payment transactions initiated at unattended terminals, where the use of strong customer authentication may not always be easy to apply due to operational reasons (e.g. to avoid queues and potential accidents at toll gates or for other safety or security risks).

12. Similar to the exemption for low-value contactless payments at the point of sale, a proper balance needs to be struck between the interest in enhanced security in remote payments and the needs of user-friendliness and accessibility of payments in the area of e-commerce. In line with those principles, thresholds below which no strong customer authentication needs to be applied should be set in a prudent manner, to cover only online purchases of low value. The thresholds for online purchases should be set more prudently, considering that the fact that the person is not physically present when making the purchase poses a slightly higher security risk.

13. The requirements of strong customer authentication apply to payments initiated by the payer, regardless of whether the payer is a natural person or a legal entity. Many corporate payments are initiated through dedicated processes or protocols which guarantee the high levels of payment security that the Payment Services Regulations 2017 (SI 2017/752) aims to achieve through strong customer authentication. Where the FCA establishes that those payment processes and protocols that are only made available to payers who are not consumers achieve the objectives of the Payment Services Regulations 2017 (SI 2017/752) in terms of security, payment service providers may, in relation to those processes or protocols, be exempted from the strong customer authentication requirements.

14. In the case of real-time transaction risk analysis that categorises a payment transaction as low risk, it is also appropriate to introduce an exemption for the payment service provider that intends not to apply strong customer authentication through the adoption of effective and risk-based requirements which ensure the safety of the payment service user's funds and personal data. Those risk-based requirements should combine the scores of the risk analysis, confirming that no abnormal spending or behavioural pattern of the payer has been identified, taking into account other risk factors including information on the location of the payer and of the payee with monetary thresholds based on fraud rates calculated for remote payments. Where, on the basis of the real-time transaction risk analysis, a payment cannot be qualified as posing a low level of risk, the payment service provider should revert to strong customer authentication. The maximum value of such risk-based exemption should be set in a manner ensuring a very low corresponding fraud rate, also by comparison to the fraud rates of all the payment transactions of the payment service provider, including those authenticated through strong customer authentication, within a certain period of time and on a rolling basis.

15. For the purpose of ensuring an effective enforcement, payment service providers that wish to benefit from the exemptions from strong customer authentication should regularly monitor and make available to the FCA upon its request, for each payment transaction type, the value of fraudulent or unauthorised payment transactions and the observed fraud rates for all their payment transactions, whether authenticated through strong customer authentication or executed under a relevant exemption.

16. The collection of this new historical evidence on the fraud rates of electronic payment transactions will also contribute to an effective review by the FCA of the thresholds for an exemption to strong customer authentication based on a real-time transaction risk analysis. The FCA should review and, if appropriate, update these Standards, including where appro-

priate the thresholds and fraud rates, with the aim of enhancing the security of remote electronic payments, on a regular basis to take account of innovation and technical developments as well as other relevant matters.

17. Payment service providers that make use of any of the exemptions to be provided for should be allowed at any time to choose to apply strong customer authentication to the actions and to the payment transactions referred to in those provisions.

18. The measures that protect the confidentiality and integrity of personalised security credentials, as well as authentication devices and software, should limit the risks relating to fraud through unauthorised or fraudulent use of payment instruments and unauthorised access to payment accounts. To this end it is necessary to introduce requirements on the secure creation and delivery of the personalised security credentials and their association with the payment service user, and to provide conditions for the renewal and deactivation of those credentials.

19. In order to ensure effective and secure communication between the relevant actors in the context of account information services, payment initiation services and confirmation on the availability of funds, it is necessary to specify the requirements of common and secure open standards of communication to be met by all relevant payment service providers. The Payment Services Regulations 2017 (SI 2017/752) provide for the access and use of payment account information by account information service providers. These Standards therefore do not change the rules of access to accounts other than payment accounts.

20. Each account servicing payment service provider with payment accounts that are accessible online should offer at least one access interface enabling secure communication with account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. The interface should enable the account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments to identify themselves to the account servicing payment service provider. It should also allow account information service providers and payment initiation service providers to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user.

FCA 2021/45 To ensure technology and business model neutrality, the account servicing payment service providers should be free to decide whether to offer an interface that is dedicated to the communication with account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments, or to allow, for that communication, the use of the interface for the identification and communication with the account servicing payment service providers' payment service users.

21. In order to allow account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments to develop their technical solutions, the technical specification of the interface should be adequately documented and made publicly available. The effect of Articles 30(3) and (5) is that the account servicing payment service provider should offer a facility enabling the payment service providers to test the technical solutions

at least six months prior to by FCA 2021/45 the date on which the interface will be launched to the market. To ensure the interoperability of different technological communication solutions, the interface should use standards of communication which are developed by international standardisation organisations.

22. The quality of the services provided by account information service providers and payment initiation service providers will depend on the proper functioning of the interfaces put in place or adapted by account servicing payment service providers. It is therefore important that in case of non-compliance of such interfaces with the provisions included in these Standards, measures are taken to guarantee business continuity for the benefit of the users of those services. It is the responsibility of the FCA to ensure that account information service providers and payment initiation service providers are not blocked or obstructed in the provision of their services.

23. Where access to payment accounts is offered by means of a dedicated interface, in order to ensure the right of payment service users to make use of payment initiation service providers and of services enabling access to account information, as provided for in the Payment Services Regulations 2017 (SI 2017/752), it is necessary to require that dedicated interfaces have the same level of availability and performance as the interface avail-

able to the payment service user. Account servicing payment service providers should also define transparent key performance indicators and service level targets for the availability and performance of dedicated interfaces that are at least as stringent as those for the interface used for their payment service users. Those interfaces should be tested by the payment service providers who will use them, and should be stress-tested and monitored by the FCA.

24. To ensure that payment service providers who rely on the dedicated interface can continue to provide their services in case of problems of availability or inadequate performance, it is necessary to provide, subject to strict conditions, a fallback mechanism that will allow such providers to use the interface that the account servicing payment service provider maintains for the identification of, and communication with, its own payment service users. Certain account servicing payment service providers will be exempted from having to provide such a fallback mechanism through their customer-facing interfaces where the FCA establishes that the dedicated interfaces comply with specific conditions that ensure unhampered competition. In the event that the exempted dedicated interfaces fail to comply with the required conditions, the granted exemptions shall be revoked by the FCA.

25. In order to allow the FCA to effectively supervise and monitor the implementation and management of the communication interfaces, the account servicing payment service providers should make a summary of the relevant documentation available on their website, and provide, upon request, the FCA with documentation of the solutions in case of emergencies. The account servicing payment service providers should also make publicly available the statistics on the availability and performance of that interface.

26. In order to safeguard the confidentiality and the integrity of data, it is necessary to ensure the security of communication sessions between account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. It is in particular necessary to require that secure encryption is applied between account information service providers, payment initiation service providers, payment service providers issuing card-based payment instruments and account servicing payment service providers when exchanging data.

27. To improve user confidence and ensure strong customer authentication, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall identify themselves to account servicing payment service providers using a form of identification issued by an independent third party. Where relevant, the use of electronic identification means and trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust service for electronic transactions in the internal market, as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 as came into force on IP completion day as defined in the EU (Withdrawal Agreement) Act 2020, should be taken into account, in particular with regard to notified electronic identification schemes.

11. Exemptions for low-value contactless payments at points of sale, which also take into account a maximum number of consecutive transactions or a certain fixed maximum value of consecutive transactions without applying strong customer authentication, allow for the development of user-friendly and low-risk payment services and should therefore be provided for. It is also appropriate to establish an exemption for the case of electronic payment transactions initiated at unattended terminals, where the use of strong customer authentication may not always be easy to apply due to operational reasons (e.g. to avoid queues and potential accidents at toll gates or for other safety or security risks).

12. Similar to the exemption for low-value contactless payments at the point of sale, a proper balance needs to be struck between the interest in enhanced security in remote payments and the needs of user-friendliness and accessibility of payments in the area of e-commerce. In line with those principles, thresholds below which no strong customer authentication needs to be applied should be set in a prudent manner, to cover only online purchases of low value. The thresholds for online purchases should be set more prudently, considering that the fact that the person is not physically present when making the purchase poses a slightly higher security risk.

13. The requirements of strong customer authentication apply to payments initiated by the payer, regardless of whether the payer is a natural person or a legal entity. Many corporate

payments are initiated through dedicated processes or protocols which guarantee the high levels of payment security that the Payment Services Regulations 2017 (SI 2017/752) aims to achieve through strong customer authentication. Where the FCA establishes that those payment processes and protocols that are only made available to payers who are not consumers achieve the objectives of the Payment Services Regulations 2017 (SI 2017/752) in terms of security, payment service providers may, in relation to those processes or protocols, be exempted from the strong customer authentication requirements.

14. In the case of real-time transaction risk analysis that categorises a payment transaction as low risk, it is also appropriate to introduce an exemption for the payment service provider that intends not to apply strong customer authentication through the adoption of effective and risk-based requirements which ensure the safety of the payment service user's funds and personal data. Those risk-based requirements should combine the scores of the risk analysis, confirming that no abnormal spending or behavioural pattern of the payer has been identified, taking into account other risk factors including information on the location of the payer and of the payee with monetary thresholds based on fraud rates calculated for remote payments. Where, on the basis of the real-time transaction risk analysis, a payment cannot be qualified as posing a low level of risk, the payment service provider should revert to strong customer authentication. The maximum value of such risk-based exemption should be set in a manner ensuring a very low corresponding fraud rate, also by comparison to the fraud rates of all the payment transactions of the payment service provider, including those authenticated through strong customer authentication, within a certain period of time and on a rolling basis.

15. For the purpose of ensuring an effective enforcement, payment service providers that wish to benefit from the exemptions from strong customer authentication should regularly monitor and make available to the FCA upon its request, for each payment transaction type, the value of fraudulent or unauthorised payment transactions and the observed fraud rates for all their payment transactions, whether authenticated through strong customer authentication or executed under a relevant exemption.

16. The collection of this new historical evidence on the fraud rates of electronic payment transactions will also contribute to an effective review by the FCA of the thresholds for an exemption to strong customer authentication based on a real-time transaction risk analysis. The FCA should review and, if appropriate, update these Standards, including where appropriate the thresholds and fraud rates, with the aim of enhancing the security of remote electronic payments, on a regular basis to take account of innovation and technical developments as well as other relevant matters.

17. Payment service providers that make use of any of the exemptions to be provided for should be allowed at any time to choose to apply strong customer authentication to the actions and to the payment transactions referred to in those provisions.

18. The measures that protect the confidentiality and integrity of personalised security credentials, as well as authentication devices and software, should limit the risks relating to fraud through unauthorised or fraudulent use of payment instruments and unauthorised access to payment accounts. To this end it is necessary to introduce requirements on the secure creation and delivery of the personalised security credentials and their association with the payment service user, and to provide conditions for the renewal and deactivation of those credentials.

19. In order to ensure effective and secure communication between the relevant actors in the context of account information services, payment initiation services and confirmation on the availability of funds, it is necessary to specify the requirements of common and secure open standards of communication to be met by all relevant payment service providers. The Payment Services Regulations 2017 (SI 2017/752) provide for the access and use of payment account information by account information service providers. These Standards therefore do not change the rules of access to accounts other than payment accounts.

20. Each account servicing payment service provider with payment accounts that are accessible online should offer at least one access interface enabling secure communication with account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. The interface should enable the account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments to identify themselves to the account servicing payment service provider. It should also allow account information service providers and payment initiation service providers to rely on the authentica-

1

tion procedures provided by the account servicing payment service provider to the payment service user.

FCA 2021/45 To ensure technology and business model neutrality, the account servicing payment service providers should be free to decide whether to offer an interface that is dedicated to the communication with account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments, or to allow, for that communication, the use of the interface for the identification and communication with the account servicing payment service providers' payment service users.

21. In order to allow account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments to develop their technical solutions, the technical specification of the interface should be adequately documented and made publicly available. The effect of Articles 30(3) and (5) is that the account servicing payment service provider should offer a facility enabling the payment service providers to test the technical solutions

at least six months prior to by FCA 2021/45 the date on which the interface will be launched to the market. To ensure the interoperability of different technological communication solutions, the interface should use standards of communication which are developed by international standardisation organisations.

22. The quality of the services provided by account information service providers and payment initiation service providers will depend on the proper functioning of the interfaces put in place or adapted by account servicing payment service providers. It is therefore important that in case of non-compliance of such interfaces with the provisions included in these Standards, measures are taken to guarantee business continuity for the benefit of the users of those services. It is the responsibility of the FCA to ensure that account information service providers and payment initiation service providers are not blocked or obstructed in the provision of their services.

23. Where access to payment accounts is offered by means of a dedicated interface, in order to ensure the right of payment service users to make use of payment initiation service providers and of services enabling access to account information, as provided for in the Payment Services Regulations 2017 (SI 2017/752), it is necessary to require that dedicated interfaces have the same level of availability and performance as the interface available to the payment service user. Account servicing payment service providers should also define transparent key performance indicators and service level targets for the availability and performance of dedicated interfaces that are at least as stringent as those for the interface used for their payment service users. Those interfaces should be tested by the payment service providers who will use them, and should be stress-tested and monitored by the FCA.

24. To ensure that payment service providers who rely on the dedicated interface can continue to provide their services in case of problems of availability or inadequate performance, it is necessary to provide, subject to strict conditions, a fallback mechanism that will allow such providers to use the interface that the account servicing payment service provider maintains for the identification of, and communication with, its own payment service users. Certain account servicing payment service providers will be exempted from having to provide such a fallback mechanism through their customer-facing interfaces where the FCA establishes that the dedicated interfaces comply with specific conditions that ensure unhampered competition. In the event that the exempted dedicated interfaces fail to comply with the required conditions, the granted exemptions shall be revoked by the FCA.

25. In order to allow the FCA to effectively supervise and monitor the implementation and management of the communication interfaces, the account servicing payment service providers should make a summary of the relevant documentation available on their website, and provide, upon request, the FCA with documentation of the solutions in case of emergencies. The account servicing payment service providers should also make publicly available the statistics on the availability and performance of that interface.

26. In order to safeguard the confidentiality and the integrity of data, it is necessary to ensure the security of communication sessions between account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. It is in particular necessary to require that secure encryption is applied between account information service providers, payment initiation service providers, payment service providers issuing card-

based payment instruments and account servicing payment service providers when exchanging data.

27. To improve user confidence and ensure strong customer authentication, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall identify themselves to account servicing payment service providers using a form of identification issued by an independent third party. Where relevant, the use of electronic identification means and trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust service for electronic transactions in the internal market, as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 as came into force on IP completion day as defined in the EU (Withdrawal Agreement) Act 2020, should be taken into account, in particular with regard to notified electronic identification schemes.

12. Similar to the exemption for low-value contactless payments at the point of sale, a proper balance needs to be struck between the interest in enhanced security in remote payments and the needs of user-friendliness and accessibility of payments in the area of e-commerce. In line with those principles, thresholds below which no strong customer authentication needs to be applied should be set in a prudent manner, to cover only online purchases of low value. The thresholds for online purchases should be set more prudently, considering that the fact that the person is not physically present when making the purchase poses a slightly higher security risk.

13. The requirements of strong customer authentication apply to payments initiated by the payer, regardless of whether the payer is a natural person or a legal entity. Many corporate payments are initiated through dedicated processes or protocols which guarantee the high levels of payment security that the Payment Services Regulations 2017 (SI 2017/752) aims to achieve through strong customer authentication. Where the FCA establishes that those payment processes and protocols that are only made available to payers who are not consumers achieve the objectives of the Payment Services Regulations 2017 (SI 2017/752) in terms of security, payment service providers may, in relation to those processes or protocols, be exempted from the strong customer authentication requirements.

14. In the case of real-time transaction risk analysis that categorises a payment transaction as low risk, it is also appropriate to introduce an exemption for the payment service provider that intends not to apply strong customer authentication through the adoption of effective and risk-based requirements which ensure the safety of the payment service user's funds and personal data. Those risk-based requirements should combine the scores of the risk analysis, confirming that no abnormal spending or behavioural pattern of the payer has been identified, taking into account other risk factors including information on the location of the payer and of the payee with monetary thresholds based on fraud rates calculated for remote payments. Where, on the basis of the real-time transaction risk analysis, a payment cannot be qualified as posing a low level of risk, the payment service provider should revert to strong customer authentication. The maximum value of such risk-based exemption should be set in a manner ensuring a very low corresponding fraud rate, also by comparison to the fraud rates of all the payment transactions of the payment service provider, including those authenticated through strong customer authentication, within a certain period of time and on a rolling basis.

15. For the purpose of ensuring an effective enforcement, payment service providers that wish to benefit from the exemptions from strong customer authentication should regularly monitor and make available to the FCA upon its request, for each payment transaction type, the value of fraudulent or unauthorised payment transactions and the observed fraud rates for all their payment transactions, whether authenticated through strong customer authentication or executed under a relevant exemption.

16. The collection of this new historical evidence on the fraud rates of electronic payment transactions will also contribute to an effective review by the FCA of the thresholds for an exemption to strong customer authentication based on a real-time transaction risk analysis. The FCA should review and, if appropriate, update these Standards, including where appropriate the thresholds and fraud rates, with the aim of enhancing the security of remote electronic payments, on a regular basis to take account of innovation and technical developments as well as other relevant matters.

17. Payment service providers that make use of any of the exemptions to be provided for should be allowed at any time to choose to apply strong customer authentication to the actions and to the payment transactions referred to in those provisions.
18. The measures that protect the confidentiality and integrity of personalised security credentials, as well as authentication devices and software, should limit the risks relating to fraud through unauthorised or fraudulent use of payment instruments and unauthorised access to payment accounts. To this end it is necessary to introduce requirements on the secure creation and delivery of the personalised security credentials and their association with the payment service user, and to provide conditions for the renewal and deactivation of those credentials.
19. In order to ensure effective and secure communication between the relevant actors in the context of account information services, payment initiation services and confirmation on the availability of funds, it is necessary to specify the requirements of common and secure open standards of communication to be met by all relevant payment service providers. The Payment Services Regulations 2017 (SI 2017/752) provide for the access and use of payment account information by account information service providers. These Standards therefore do not change the rules of access to accounts other than payment accounts.
20. Each account servicing payment service provider with payment accounts that are accessible online should offer at least one access interface enabling secure communication with account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. The interface should enable the account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments to identify themselves to the account servicing payment service provider. It should also allow account information service providers and payment initiation service providers to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user.
FCA 2021/45 To ensure technology and business model neutrality, the account servicing payment service providers should be free to decide whether to offer an interface that is dedicated to the communication with account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments, or to allow, for that communication, the use of the interface for the identification and communication with the account servicing payment service providers' payment service users.
21. In order to allow account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments to develop their technical solutions, the technical specification of the interface should be adequately documented and made publicly available. The effect of Articles 30(3) and (5) is that the account servicing payment service provider should offer a facility enabling the payment service providers to test the technical solutions
at least six months prior to by FCA 2021/45 the date on which the interface will be launched to the market. To ensure the interoperability of different technological communication solutions, the interface should use standards of communication which are developed by international standardisation organisations.
22. The quality of the services provided by account information service providers and payment initiation service providers will depend on the proper functioning of the interfaces put in place or adapted by account servicing payment service providers. It is therefore important that in case of non-compliance of such interfaces with the provisions included in these Standards, measures are taken to guarantee business continuity for the benefit of the users of those services. It is the responsibility of the FCA to ensure that account information service providers and payment initiation service providers are not blocked or obstructed in the provision of their services.
23. Where access to payment accounts is offered by means of a dedicated interface, in order to ensure the right of payment service users to make use of payment initiation service providers and of services enabling access to account information, as provided for in the Payment Services Regulations 2017 (SI 2017/752), it is necessary to require that dedicated interfaces have the same level of availability and performance as the interface available to the payment service user. Account servicing payment service providers should also define transparent key performance indicators and service level targets for the availability and performance of dedicated interfaces that are at least as stringent as those for the inter-

face used for their payment service users. Those interfaces should be tested by the payment service providers who will use them, and should be stress-tested and monitored by the FCA.
24. To ensure that payment service providers who rely on the dedicated interface can continue to provide their services in case of problems of availability or inadequate performance, it is necessary to provide, subject to strict conditions, a fallback mechanism that will allow such providers to use the interface that the account servicing payment service provider maintains for the identification of, and communication with, its own payment service users. Certain account servicing payment service providers will be exempted from having to provide such a fallback mechanism through their customer-facing interfaces where the FCA establishes that the dedicated interfaces comply with specific conditions that ensure unhampered competition. In the event that the exempted dedicated interfaces fail to comply with the required conditions, the granted exemptions shall be revoked by the FCA.
25. In order to allow the FCA to effectively supervise and monitor the implementation and management of the communication interfaces, the account servicing payment service providers should make a summary of the relevant documentation available on their website, and provide, upon request, the FCA with documentation of the solutions in case of emergencies. The account servicing payment service providers should also make publicly available the statistics on the availability and performance of that interface.
26. In order to safeguard the confidentiality and the integrity of data, it is necessary to ensure the security of communication sessions between account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. It is in particular necessary to require that secure encryption is applied between account information service providers, payment initiation service providers, payment service providers issuing card-based payment instruments and account servicing payment service providers when exchanging data.
27. To improve user confidence and ensure strong customer authentication, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall identify themselves to account servicing payment service providers using a form of identification issued by an independent third party. Where relevant, the use of electronic identification means and trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust service for electronic transactions in the internal market, as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 as came into force on IP completion day as defined in the EU (Withdrawal Agreement) Act 2020, should be taken into account, in particular with regard to notified electronic identification schemes.

13. The requirements of strong customer authentication apply to payments initiated by the payer, regardless of whether the payer is a natural person or a legal entity. Many corporate payments are initiated through dedicated processes or protocols which guarantee the high levels of payment security that the Payment Services Regulations 2017 (SI 2017/752) aims to achieve through strong customer authentication. Where the FCA establishes that those payment processes and protocols that are only made available to payers who are not consumers achieve the objectives of the Payment Services Regulations 2017 (SI 2017/752) in terms of security, payment service providers may, in relation to those processes or protocols, be exempted from the strong customer authentication requirements.
14. In the case of real-time transaction risk analysis that categorises a payment transaction as low risk, it is also appropriate to introduce an exemption for the payment service provider that intends not to apply strong customer authentication through the adoption of effective and risk-based requirements which ensure the safety of the payment service user's funds and personal data. Those risk-based requirements should combine the scores of the risk analysis, confirming that no abnormal spending or behavioural pattern of the payer has been identified, taking into account other risk factors including information on the location of the payer and of the payee with monetary thresholds based on fraud rates calculated for remote payments. Where, on the basis of the real-time transaction risk analysis, a payment cannot be qualified as posing a low level of risk, the payment service provider should revert to strong customer authentication. The maximum value of such risk-based exemption should be set in a manner ensuring a very low corresponding fraud rate, also by comparison to the

1

fraud rates of all the payment transactions of the payment service provider, including those authenticated through strong customer authentication, within a certain period of time and on a rolling basis.

15. For the purpose of ensuring an effective enforcement, payment service providers that wish to benefit from the exemptions from strong customer authentication should regularly monitor and make available to the FCA upon its request, for each payment transaction type, the value of fraudulent or unauthorised payment transactions and the observed fraud rates for all their payment transactions, whether authenticated through strong customer authentication or executed under a relevant exemption.

16. The collection of this new historical evidence on the fraud rates of electronic payment transactions will also contribute to an effective review by the FCA of the thresholds for an exemption to strong customer authentication based on a real-time transaction risk analysis. The FCA should review and, if appropriate, update these Standards, including where appropriate the thresholds and fraud rates, with the aim of enhancing the security of remote electronic payments, on a regular basis to take account of innovation and technical developments as well as other relevant matters.

17. Payment service providers that make use of any of the exemptions to be provided for should be allowed at any time to choose to apply strong customer authentication to the actions and to the payment transactions referred to in those provisions.

18. The measures that protect the confidentiality and integrity of personalised security credentials, as well as authentication devices and software, should limit the risks relating to fraud through unauthorised or fraudulent use of payment instruments and unauthorised access to payment accounts. To this end it is necessary to introduce requirements on the secure creation and delivery of the personalised security credentials and their association with the payment service user, and to provide conditions for the renewal and deactivation of those credentials.

19. In order to ensure effective and secure communication between the relevant actors in the context of account information services, payment initiation services and confirmation on the availability of funds, it is necessary to specify the requirements of common and secure open standards of communication to be met by all relevant payment service providers. The Payment Services Regulations 2017 (SI 2017/752) provide for the access and use of payment account information by account information service providers. These Standards therefore do not change the rules of access to accounts other than payment accounts.

20. Each account servicing payment service provider with payment accounts that are accessible online should offer at least one access interface enabling secure communication with account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. The interface should enable the account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments to identify themselves to the account servicing payment service provider. It should also allow account information service providers and payment initiation service providers to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user.

FCA 2021/45 To ensure technology and business model neutrality, the account servicing payment service providers should be free to decide whether to offer an interface that is dedicated to the communication with account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments, or to allow, for that communication, the use of the interface for the identification and communication with the account servicing payment service providers' payment service users.

21. In order to allow account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments to develop their technical solutions, the technical specification of the interface should be adequately documented and made publicly available. The effect of Articles 30(3) and (5) is that the account servicing payment service provider should offer a facility enabling the payment service providers to test the technical solutions

at least six months prior to by FCA 2021/45 the date on which the interface will be launched to the market. To ensure the interoperability of different technological communication solutions, the interface should use standards of communication which are developed by international standardisation organisations.

22. The quality of the services provided by account information service providers and payment initiation service providers will depend on the proper functioning of the interfaces put in place or adapted by account servicing payment service providers. It is therefore important that in case of non-compliance of such interfaces with the provisions included in these Standards, measures are taken to guarantee business continuity for the benefit of the users of those services. It is the responsibility of the FCA to ensure that account information service providers and payment initiation service providers are not blocked or obstructed in the provision of their services.
23. Where access to payment accounts is offered by means of a dedicated interface, in order to ensure the right of payment service users to make use of payment initiation service providers and of services enabling access to account information, as provided for in the Payment Services Regulations 2017 (SI 2017/752), it is necessary to require that dedicated interfaces have the same level of availability and performance as the interface available to the payment service user. Account servicing payment service providers should also define transparent key performance indicators and service level targets for the availability and performance of dedicated interfaces that are at least as stringent as those for the interface used for their payment service users. Those interfaces should be tested by the payment service providers who will use them, and should be stress-tested and monitored by the FCA.
24. To ensure that payment service providers who rely on the dedicated interface can continue to provide their services in case of problems of availability or inadequate performance, it is necessary to provide, subject to strict conditions, a fallback mechanism that will allow such providers to use the interface that the account servicing payment service provider maintains for the identification of, and communication with, its own payment service users. Certain account servicing payment service providers will be exempted from having to provide such a fallback mechanism through their customer-facing interfaces where the FCA establishes that the dedicated interfaces comply with specific conditions that ensure unhampered competition. In the event that the exempted dedicated interfaces fail to comply with the required conditions, the granted exemptions shall be revoked by the FCA.
25. In order to allow the FCA to effectively supervise and monitor the implementation and management of the communication interfaces, the account servicing payment service providers should make a summary of the relevant documentation available on their website, and provide, upon request, the FCA with documentation of the solutions in case of emergencies. The account servicing payment service providers should also make publicly available the statistics on the availability and performance of that interface.
26. In order to safeguard the confidentiality and the integrity of data, it is necessary to ensure the security of communication sessions between account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. It is in particular necessary to require that secure encryption is applied between account information service providers, payment initiation service providers, payment service providers issuing card-based payment instruments and account servicing payment service providers when exchanging data.
27. To improve user confidence and ensure strong customer authentication, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall identify themselves to account servicing payment service providers using a form of identification issued by an independent third party. Where relevant, the use of electronic identification means and trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust service for electronic transactions in the internal market, as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 as came into force on IP completion day as defined in the EU (Withdrawal Agreement) Act 2020, should be taken into account, in particular with regard to notified electronic identification schemes.

14. In the case of real-time transaction risk analysis that categorises a payment transaction as low risk, it is also appropriate to introduce an exemption for the payment service provider that intends not to apply strong customer authentication through the adoption of effective and risk-based requirements which ensure the safety of the payment service user's funds and personal data. Those risk-based requirements should combine the scores of the risk

1

analysis, confirming that no abnormal spending or behavioural pattern of the payer has been identified, taking into account other risk factors including information on the location of the payer and of the payee with monetary thresholds based on fraud rates calculated for remote payments. Where, on the basis of the real-time transaction risk analysis, a payment cannot be qualified as posing a low level of risk, the payment service provider should revert to strong customer authentication. The maximum value of such risk-based exemption should be set in a manner ensuring a very low corresponding fraud rate, also by comparison to the fraud rates of all the payment transactions of the payment service provider, including those authenticated through strong customer authentication, within a certain period of time and on a rolling basis.

15. For the purpose of ensuring an effective enforcement, payment service providers that wish to benefit from the exemptions from strong customer authentication should regularly monitor and make available to the FCA upon its request, for each payment transaction type, the value of fraudulent or unauthorised payment transactions and the observed fraud rates for all their payment transactions, whether authenticated through strong customer authentication or executed under a relevant exemption.

16. The collection of this new historical evidence on the fraud rates of electronic payment transactions will also contribute to an effective review by the FCA of the thresholds for an exemption to strong customer authentication based on a real-time transaction risk analysis. The FCA should review and, if appropriate, update these Standards, including where appropriate the thresholds and fraud rates, with the aim of enhancing the security of remote electronic payments, on a regular basis to take account of innovation and technical developments as well as other relevant matters.

17. Payment service providers that make use of any of the exemptions to be provided for should be allowed at any time to choose to apply strong customer authentication to the actions and to the payment transactions referred to in those provisions.

18. The measures that protect the confidentiality and integrity of personalised security credentials, as well as authentication devices and software, should limit the risks relating to fraud through unauthorised or fraudulent use of payment instruments and unauthorised access to payment accounts. To this end it is necessary to introduce requirements on the secure creation and delivery of the personalised security credentials and their association with the payment service user, and to provide conditions for the renewal and deactivation of those credentials.

19. In order to ensure effective and secure communication between the relevant actors in the context of account information services, payment initiation services and confirmation on the availability of funds, it is necessary to specify the requirements of common and secure open standards of communication to be met by all relevant payment service providers. The Payment Services Regulations 2017 (SI 2017/752) provide for the access and use of payment account information by account information service providers. These Standards therefore do not change the rules of access to accounts other than payment accounts.

20. Each account servicing payment service provider with payment accounts that are accessible online should offer at least one access interface enabling secure communication with account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. The interface should enable the account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments to identify themselves to the account servicing payment service provider. It should also allow account information service providers and payment initiation service providers to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user.

FCA 2021/45 To ensure technology and business model neutrality, the account servicing payment service providers should be free to decide whether to offer an interface that is dedicated to the communication with account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments, or to allow, for that communication, the use of the interface for the identification and communication with the account servicing payment service providers' payment service users.

21. In order to allow account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments to develop their technical solutions, the technical specification of the interface should be

adequately documented and made publicly available. The effect of Articles 30(3) and (5) is that the account servicing payment service provider should offer a facility enabling the payment service providers to test the technical solutions
at least six months prior to by FCA 2021/45 the date on which the interface will be launched to the market. To ensure the interoperability of different technological communication solutions, the interface should use standards of communication which are developed by international standardisation organisations.

22. The quality of the services provided by account information service providers and payment initiation service providers will depend on the proper functioning of the interfaces put in place or adapted by account servicing payment service providers. It is therefore important that in case of non-compliance of such interfaces with the provisions included in these Standards, measures are taken to guarantee business continuity for the benefit of the users of those services. It is the responsibility of the FCA to ensure that account information service providers and payment initiation service providers are not blocked or obstructed in the provision of their services.

23. Where access to payment accounts is offered by means of a dedicated interface, in order to ensure the right of payment service users to make use of payment initiation service providers and of services enabling access to account information, as provided for in the Payment Services Regulations 2017 (SI 2017/752), it is necessary to require that dedicated interfaces have the same level of availability and performance as the interface available to the payment service user. Account servicing payment service providers should also define transparent key performance indicators and service level targets for the availability and performance of dedicated interfaces that are at least as stringent as those for the interface used for their payment service users. Those interfaces should be tested by the payment service providers who will use them, and should be stress-tested and monitored by the FCA.

24. To ensure that payment service providers who rely on the dedicated interface can continue to provide their services in case of problems of availability or inadequate performance, it is necessary to provide, subject to strict conditions, a fallback mechanism that will allow such providers to use the interface that the account servicing payment service provider maintains for the identification of, and communication with, its own payment service users. Certain account servicing payment service providers will be exempted from having to provide such a fallback mechanism through their customer-facing interfaces where the FCA establishes that the dedicated interfaces comply with specific conditions that ensure unhampered competition. In the event that the exempted dedicated interfaces fail to comply with the required conditions, the granted exemptions shall be revoked by the FCA.

25. In order to allow the FCA to effectively supervise and monitor the implementation and management of the communication interfaces, the account servicing payment service providers should make a summary of the relevant documentation available on their website, and provide, upon request, the FCA with documentation of the solutions in case of emergencies. The account servicing payment service providers should also make publicly available the statistics on the availability and performance of that interface.

26. In order to safeguard the confidentiality and the integrity of data, it is necessary to ensure the security of communication sessions between account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. It is in particular necessary to require that secure encryption is applied between account information service providers, payment initiation service providers, payment service providers issuing card-based payment instruments and account servicing payment service providers when exchanging data.

27. To improve user confidence and ensure strong customer authentication, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall identify themselves to account servicing payment service providers using a form of identification issued by an independent third party. Where relevant, the use of electronic identification means and trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust service for electronic transactions in the internal market, as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 as came into force on IP completion

1

day as defined in the EU (Withdrawal Agreement) Act 2020, should be taken into account, in particular with regard to notified electronic identification schemes.

15. For the purpose of ensuring an effective enforcement, payment service providers that wish to benefit from the exemptions from strong customer authentication should regularly monitor and make available to the FCA upon its request, for each payment transaction type, the value of fraudulent or unauthorised payment transactions and the observed fraud rates for all their payment transactions, whether authenticated through strong customer authentication or executed under a relevant exemption.

16. The collection of this new historical evidence on the fraud rates of electronic payment transactions will also contribute to an effective review by the FCA of the thresholds for an exemption to strong customer authentication based on a real-time transaction risk analysis. The FCA should review and, if appropriate, update these Standards, including where appropriate the thresholds and fraud rates, with the aim of enhancing the security of remote electronic payments, on a regular basis to take account of innovation and technical developments as well as other relevant matters.

17. Payment service providers that make use of any of the exemptions to be provided for should be allowed at any time to choose to apply strong customer authentication to the actions and to the payment transactions referred to in those provisions.

18. The measures that protect the confidentiality and integrity of personalised security credentials, as well as authentication devices and software, should limit the risks relating to fraud through unauthorised or fraudulent use of payment instruments and unauthorised access to payment accounts. To this end it is necessary to introduce requirements on the secure creation and delivery of the personalised security credentials and their association with the payment service user, and to provide conditions for the renewal and deactivation of those credentials.

19. In order to ensure effective and secure communication between the relevant actors in the context of account information services, payment initiation services and confirmation on the availability of funds, it is necessary to specify the requirements of common and secure open standards of communication to be met by all relevant payment service providers. The Payment Services Regulations 2017 (SI 2017/752) provide for the access and use of payment account information by account information service providers. These Standards therefore do not change the rules of access to accounts other than payment accounts.

20. Each account servicing payment service provider with payment accounts that are accessible online should offer at least one access interface enabling secure communication with account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. The interface should enable the account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments to identify themselves to the account servicing payment service provider. It should also allow account information service providers and payment initiation service providers to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user.

FCA 2021/45 To ensure technology and business model neutrality, the account servicing payment service providers should be free to decide whether to offer an interface that is dedicated to the communication with account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments, or to allow, for that communication, the use of the interface for the identification and communication with the account servicing payment service providers' payment service users.

21. In order to allow account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments to develop their technical solutions, the technical specification of the interface should be adequately documented and made publicly available. The effect of Articles 30(3) and (5) is that the account servicing payment service provider should offer a facility enabling the payment service providers to test the technical solutions

at least six months prior to by FCA 2021/45 the date on which the interface will be launched to the market. To ensure the interoperability of different technological communic-

ation solutions, the interface should use standards of communication which are developed by international standardisation organisations.

22. The quality of the services provided by account information service providers and payment initiation service providers will depend on the proper functioning of the interfaces put in place or adapted by account servicing payment service providers. It is therefore important that in case of non-compliance of such interfaces with the provisions included in these Standards, measures are taken to guarantee business continuity for the benefit of the users of those services. It is the responsibility of the FCA to ensure that account information service providers and payment initiation service providers are not blocked or obstructed in the provision of their services.

23. Where access to payment accounts is offered by means of a dedicated interface, in order to ensure the right of payment service users to make use of payment initiation service providers and of services enabling access to account information, as provided for in the Payment Services Regulations 2017 (SI 2017/752), it is necessary to require that dedicated interfaces have the same level of availability and performance as the interface available to the payment service user. Account servicing payment service providers should also define transparent key performance indicators and service level targets for the availability and performance of dedicated interfaces that are at least as stringent as those for the interface used for their payment service users. Those interfaces should be tested by the payment service providers who will use them, and should be stress-tested and monitored by the FCA.

24. To ensure that payment service providers who rely on the dedicated interface can continue to provide their services in case of problems of availability or inadequate performance, it is necessary to provide, subject to strict conditions, a fallback mechanism that will allow such providers to use the interface that the account servicing payment service provider maintains for the identification of, and communication with, its own payment service users. Certain account servicing payment service providers will be exempted from having to provide such a fallback mechanism through their customer-facing interfaces where the FCA establishes that the dedicated interfaces comply with specific conditions that ensure unhampered competition. In the event that the exempted dedicated interfaces fail to comply with the required conditions, the granted exemptions shall be revoked by the FCA.

25. In order to allow the FCA to effectively supervise and monitor the implementation and management of the communication interfaces, the account servicing payment service providers should make a summary of the relevant documentation available on their website, and provide, upon request, the FCA with documentation of the solutions in case of emergencies. The account servicing payment service providers should also make publicly available the statistics on the availability and performance of that interface.

26. In order to safeguard the confidentiality and the integrity of data, it is necessary to ensure the security of communication sessions between account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. It is in particular necessary to require that secure encryption is applied between account information service providers, payment initiation service providers, payment service providers issuing card-based payment instruments and account servicing payment service providers when exchanging data.

27. To improve user confidence and ensure strong customer authentication, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall identify themselves to account servicing payment service providers using a form of identification issued by an independent third party. Where relevant, the use of electronic identification means and trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust service for electronic transactions in the internal market, as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 as came into force on IP completion day as defined in the EU (Withdrawal Agreement) Act 2020, should be taken into account, in particular with regard to notified electronic identification schemes.

16. The collection of this new historical evidence on the fraud rates of electronic payment transactions will also contribute to an effective review by the FCA of the thresholds for an exemption to strong customer authentication based on a real-time transaction risk analysis.

1

The FCA should review and, if appropriate, update these Standards, including where appropriate the thresholds and fraud rates, with the aim of enhancing the security of remote electronic payments, on a regular basis to take account of innovation and technical developments as well as other relevant matters.

17. Payment service providers that make use of any of the exemptions to be provided for should be allowed at any time to choose to apply strong customer authentication to the actions and to the payment transactions referred to in those provisions.

18. The measures that protect the confidentiality and integrity of personalised security credentials, as well as authentication devices and software, should limit the risks relating to fraud through unauthorised or fraudulent use of payment instruments and unauthorised access to payment accounts. To this end it is necessary to introduce requirements on the secure creation and delivery of the personalised security credentials and their association with the payment service user, and to provide conditions for the renewal and deactivation of those credentials.

19. In order to ensure effective and secure communication between the relevant actors in the context of account information services, payment initiation services and confirmation on the availability of funds, it is necessary to specify the requirements of common and secure open standards of communication to be met by all relevant payment service providers. The Payment Services Regulations 2017 (SI 2017/752) provide for the access and use of payment account information by account information service providers. These Standards therefore do not change the rules of access to accounts other than payment accounts.

20. Each account servicing payment service provider with payment accounts that are accessible online should offer at least one access interface enabling secure communication with account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. The interface should enable the account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments to identify themselves to the account servicing payment service provider. It should also allow account information service providers and payment initiation service providers to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user.

FCA 2021/45 To ensure technology and business model neutrality, the account servicing payment service providers should be free to decide whether to offer an interface that is dedicated to the communication with account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments, or to allow, for that communication, the use of the interface for the identification and communication with the account servicing payment service providers' payment service users.

21. In order to allow account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments to develop their technical solutions, the technical specification of the interface should be adequately documented and made publicly available. The effect of Articles 30(3) and (5) is that the account servicing payment service provider should offer a facility enabling the payment service providers to test the technical solutions

at least six months prior to by FCA 2021/45 the date on which the interface will be launched to the market. To ensure the interoperability of different technological communication solutions, the interface should use standards of communication which are developed by international standardisation organisations.

22. The quality of the services provided by account information service providers and payment initiation service providers will depend on the proper functioning of the interfaces put in place or adapted by account servicing payment service providers. It is therefore important that in case of non-compliance of such interfaces with the provisions included in these Standards, measures are taken to guarantee business continuity for the benefit of the users of those services. It is the responsibility of the FCA to ensure that account information service providers and payment initiation service providers are not blocked or obstructed in the provision of their services.

23. Where access to payment accounts is offered by means of a dedicated interface, in order to ensure the right of payment service users to make use of payment initiation service providers and of services enabling access to account information, as provided for in the Payment Services Regulations 2017 (SI 2017/752), it is necessary to require that dedic-

ated interfaces have the same level of availability and performance as the interface available to the payment service user. Account servicing payment service providers should also define transparent key performance indicators and service level targets for the availability and performance of dedicated interfaces that are at least as stringent as those for the interface used for their payment service users. Those interfaces should be tested by the payment service providers who will use them, and should be stress-tested and monitored by the FCA.

24. To ensure that payment service providers who rely on the dedicated interface can continue to provide their services in case of problems of availability or inadequate performance, it is necessary to provide, subject to strict conditions, a fallback mechanism that will allow such providers to use the interface that the account servicing payment service provider maintains for the identification of, and communication with, its own payment service users. Certain account servicing payment service providers will be exempted from having to provide such a fallback mechanism through their customer-facing interfaces where the FCA establishes that the dedicated interfaces comply with specific conditions that ensure unhampered competition. In the event that the exempted dedicated interfaces fail to comply with the required conditions, the granted exemptions shall be revoked by the FCA.

25. In order to allow the FCA to effectively supervise and monitor the implementation and management of the communication interfaces, the account servicing payment service providers should make a summary of the relevant documentation available on their website, and provide, upon request, the FCA with documentation of the solutions in case of emergencies. The account servicing payment service providers should also make publicly available the statistics on the availability and performance of that interface.

26. In order to safeguard the confidentiality and the integrity of data, it is necessary to ensure the security of communication sessions between account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. It is in particular necessary to require that secure encryption is applied between account information service providers, payment initiation service providers, payment service providers issuing card-based payment instruments and account servicing payment service providers when exchanging data.

27. To improve user confidence and ensure strong customer authentication, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall identify themselves to account servicing payment service providers using a form of identification issued by an independent third party. Where relevant, the use of electronic identification means and trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust service for electronic transactions in the internal market, as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 as came into force on IP completion day as defined in the EU (Withdrawal Agreement) Act 2020, should be taken into account, in particular with regard to notified electronic identification schemes.

17. Payment service providers that make use of any of the exemptions to be provided for should be allowed at any time to choose to apply strong customer authentication to the actions and to the payment transactions referred to in those provisions.

18. The measures that protect the confidentiality and integrity of personalised security credentials, as well as authentication devices and software, should limit the risks relating to fraud through unauthorised or fraudulent use of payment instruments and unauthorised access to payment accounts. To this end it is necessary to introduce requirements on the secure creation and delivery of the personalised security credentials and their association with the payment service user, and to provide conditions for the renewal and deactivation of those credentials.

19. In order to ensure effective and secure communication between the relevant actors in the context of account information services, payment initiation services and confirmation on the availability of funds, it is necessary to specify the requirements of common and secure open standards of communication to be met by all relevant payment service providers. The Payment Services Regulations 2017 (SI 2017/752) provide for the access and use of payment account information by account information service providers. These Standards therefore do not change the rules of access to accounts other than payment accounts.

20. Each account servicing payment service provider with payment accounts that are accessible online should offer at least one access interface enabling secure communication with account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. The interface should enable the account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments to identify themselves to the account servicing payment service provider. It should also allow account information service providers and payment initiation service providers to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user.

FCA 2021/45 To ensure technology and business model neutrality, the account servicing payment service providers should be free to decide whether to offer an interface that is dedicated to the communication with account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments, or to allow, for that communication, the use of the interface for the identification and communication with the account servicing payment service providers' payment service users.

21. In order to allow account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments to develop their technical solutions, the technical specification of the interface should be adequately documented and made publicly available. The effect of Articles 30(3) and (5) is that the account servicing payment service provider should offer a facility enabling the payment service providers to test the technical solutions

at least six months prior to by FCA 2021/45 the date on which the interface will be launched to the market. To ensure the interoperability of different technological communication solutions, the interface should use standards of communication which are developed by international standardisation organisations.

22. The quality of the services provided by account information service providers and payment initiation service providers will depend on the proper functioning of the interfaces put in place or adapted by account servicing payment service providers. It is therefore important that in case of non-compliance of such interfaces with the provisions included in these Standards, measures are taken to guarantee business continuity for the benefit of the users of those services. It is the responsibility of the FCA to ensure that account information service providers and payment initiation service providers are not blocked or obstructed in the provision of their services.

23. Where access to payment accounts is offered by means of a dedicated interface, in order to ensure the right of payment service users to make use of payment initiation service providers and of services enabling access to account information, as provided for in the Payment Services Regulations 2017 (SI 2017/752), it is necessary to require that dedicated interfaces have the same level of availability and performance as the interface available to the payment service user. Account servicing payment service providers should also define transparent key performance indicators and service level targets for the availability and performance of dedicated interfaces that are at least as stringent as those for the interface used for their payment service users. Those interfaces should be tested by the payment service providers who will use them, and should be stress-tested and monitored by the FCA.

24. To ensure that payment service providers who rely on the dedicated interface can continue to provide their services in case of problems of availability or inadequate performance, it is necessary to provide, subject to strict conditions, a fallback mechanism that will allow such providers to use the interface that the account servicing payment service provider maintains for the identification of, and communication with, its own payment service users. Certain account servicing payment service providers will be exempted from having to provide such a fallback mechanism through their customer-facing interfaces where the FCA establishes that the dedicated interfaces comply with specific conditions that ensure unhampered competition. In the event that the exempted dedicated interfaces fail to comply with the required conditions, the granted exemptions shall be revoked by the FCA.

25. In order to allow the FCA to effectively supervise and monitor the implementation and management of the communication interfaces, the account servicing payment service providers should make a summary of the relevant documentation available on their website, and provide, upon request, the FCA with documentation of the solutions in case of emer-

gencies. The account servicing payment service providers should also make publicly available the statistics on the availability and performance of that interface.

26. In order to safeguard the confidentiality and the integrity of data, it is necessary to ensure the security of communication sessions between account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. It is in particular necessary to require that secure encryption is applied between account information service providers, payment initiation service providers, payment service providers issuing card-based payment instruments and account servicing payment service providers when exchanging data.

27. To improve user confidence and ensure strong customer authentication, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall identify themselves to account servicing payment service providers using a form of identification issued by an independent third party. Where relevant, the use of electronic identification means and trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust service for electronic transactions in the internal market, as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 as came into force on IP completion day as defined in the EU (Withdrawal Agreement) Act 2020, should be taken into account, in particular with regard to notified electronic identification schemes.

18. The measures that protect the confidentiality and integrity of personalised security credentials, as well as authentication devices and software, should limit the risks relating to fraud through unauthorised or fraudulent use of payment instruments and unauthorised access to payment accounts. To this end it is necessary to introduce requirements on the secure creation and delivery of the personalised security credentials and their association with the payment service user, and to provide conditions for the renewal and deactivation of those credentials.

19. In order to ensure effective and secure communication between the relevant actors in the context of account information services, payment initiation services and confirmation on the availability of funds, it is necessary to specify the requirements of common and secure open standards of communication to be met by all relevant payment service providers. The Payment Services Regulations 2017 (SI 2017/752) provide for the access and use of payment account information by account information service providers. These Standards therefore do not change the rules of access to accounts other than payment accounts.

20. Each account servicing payment service provider with payment accounts that are accessible online should offer at least one access interface enabling secure communication with account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. The interface should enable the account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments to identify themselves to the account servicing payment service provider. It should also allow account information service providers and payment initiation service providers to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user.

FCA 2021/45 To ensure technology and business model neutrality, the account servicing payment service providers should be free to decide whether to offer an interface that is dedicated to the communication with account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments, or to allow, for that communication, the use of the interface for the identification and communication with the account servicing payment service providers' payment service users.

21. In order to allow account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments to develop their technical solutions, the technical specification of the interface should be adequately documented and made publicly available. The effect of Articles 30(3) and (5) is that the account servicing payment service provider should offer a facility enabling the payment service providers to test the technical solutions

1

at least six months prior to by FCA 2021/45 the date on which the interface will be launched to the market. To ensure the interoperability of different technological communication solutions, the interface should use standards of communication which are developed by international standardisation organisations.

22. The quality of the services provided by account information service providers and payment initiation service providers will depend on the proper functioning of the interfaces put in place or adapted by account servicing payment service providers. It is therefore important that in case of non-compliance of such interfaces with the provisions included in these Standards, measures are taken to guarantee business continuity for the benefit of the users of those services. It is the responsibility of the FCA to ensure that account information service providers and payment initiation service providers are not blocked or obstructed in the provision of their services.

23. Where access to payment accounts is offered by means of a dedicated interface, in order to ensure the right of payment service users to make use of payment initiation service providers and of services enabling access to account information, as provided for in the Payment Services Regulations 2017 (SI 2017/752), it is necessary to require that dedicated interfaces have the same level of availability and performance as the interface available to the payment service user. Account servicing payment service providers should also define transparent key performance indicators and service level targets for the availability and performance of dedicated interfaces that are at least as stringent as those for the interface used for their payment service users. Those interfaces should be tested by the payment service providers who will use them, and should be stress-tested and monitored by the FCA.

24. To ensure that payment service providers who rely on the dedicated interface can continue to provide their services in case of problems of availability or inadequate performance, it is necessary to provide, subject to strict conditions, a fallback mechanism that will allow such providers to use the interface that the account servicing payment service provider maintains for the identification of, and communication with, its own payment service users. Certain account servicing payment service providers will be exempted from having to provide such a fallback mechanism through their customer-facing interfaces where the FCA establishes that the dedicated interfaces comply with specific conditions that ensure unhampered competition. In the event that the exempted dedicated interfaces fail to comply with the required conditions, the granted exemptions shall be revoked by the FCA.

25. In order to allow the FCA to effectively supervise and monitor the implementation and management of the communication interfaces, the account servicing payment service providers should make a summary of the relevant documentation available on their website, and provide, upon request, the FCA with documentation of the solutions in case of emergencies. The account servicing payment service providers should also make publicly available the statistics on the availability and performance of that interface.

26. In order to safeguard the confidentiality and the integrity of data, it is necessary to ensure the security of communication sessions between account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. It is in particular necessary to require that secure encryption is applied between account information service providers, payment initiation service providers, payment service providers issuing card-based payment instruments and account servicing payment service providers when exchanging data.

27. To improve user confidence and ensure strong customer authentication, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall identify themselves to account servicing payment service providers using a form of identification issued by an independent third party. Where relevant, the use of electronic identification means and trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust service for electronic transactions in the internal market, as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 as came into force on IP completion day as defined in the EU (Withdrawal Agreement) Act 2020, should be taken into account, in particular with regard to notified electronic identification schemes.

19. In order to ensure effective and secure communication between the relevant actors in the context of account information services, payment initiation services and confirmation on the availability of funds, it is necessary to specify the requirements of common and secure open standards of communication to be met by all relevant payment service providers. The Payment Services Regulations 2017 (SI 2017/752) provide for the access and use of payment account information by account information service providers. These Standards therefore do not change the rules of access to accounts other than payment accounts.

20. Each account servicing payment service provider with payment accounts that are accessible online should offer at least one access interface enabling secure communication with account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. The interface should enable the account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments to identify themselves to the account servicing payment service provider. It should also allow account information service providers and payment initiation service providers to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user.

FCA 2021/45 To ensure technology and business model neutrality, the account servicing payment service providers should be free to decide whether to offer an interface that is dedicated to the communication with account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments, or to allow, for that communication, the use of the interface for the identification and communication with the account servicing payment service providers' payment service users.

21. In order to allow account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments to develop their technical solutions, the technical specification of the interface should be adequately documented and made publicly available. The effect of Articles 30(3) and (5) is that the account servicing payment service provider should offer a facility enabling the payment service providers to test the technical solutions

at least six months prior to by FCA 2021/45 the date on which the interface will be launched to the market. To ensure the interoperability of different technological communication solutions, the interface should use standards of communication which are developed by international standardisation organisations.

22. The quality of the services provided by account information service providers and payment initiation service providers will depend on the proper functioning of the interfaces put in place or adapted by account servicing payment service providers. It is therefore important that in case of non-compliance of such interfaces with the provisions included in these Standards, measures are taken to guarantee business continuity for the benefit of the users of those services. It is the responsibility of the FCA to ensure that account information service providers and payment initiation service providers are not blocked or obstructed in the provision of their services.

23. Where access to payment accounts is offered by means of a dedicated interface, in order to ensure the right of payment service users to make use of payment initiation service providers and of services enabling access to account information, as provided for in the Payment Services Regulations 2017 (SI 2017/752), it is necessary to require that dedicated interfaces have the same level of availability and performance as the interface available to the payment service user. Account servicing payment service providers should also define transparent key performance indicators and service level targets for the availability and performance of dedicated interfaces that are at least as stringent as those for the interface used for their payment service users. Those interfaces should be tested by the payment service providers who will use them, and should be stress-tested and monitored by the FCA.

24. To ensure that payment service providers who rely on the dedicated interface can continue to provide their services in case of problems of availability or inadequate performance, it is necessary to provide, subject to strict conditions, a fallback mechanism that will allow such providers to use the interface that the account servicing payment service provider maintains for the identification of, and communication with, its own payment service users. Certain account servicing payment service providers will be exempted from having to provide such a fallback mechanism through their customer-facing interfaces where the FCA establishes that the dedicated interfaces comply with specific conditions that ensure

1

unhampered competition. In the event that the exempted dedicated interfaces fail to comply with the required conditions, the granted exemptions shall be revoked by the FCA.

25. In order to allow the FCA to effectively supervise and monitor the implementation and management of the communication interfaces, the account servicing payment service providers should make a summary of the relevant documentation available on their website, and provide, upon request, the FCA with documentation of the solutions in case of emergencies. The account servicing payment service providers should also make publicly available the statistics on the availability and performance of that interface.

26. In order to safeguard the confidentiality and the integrity of data, it is necessary to ensure the security of communication sessions between account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. It is in particular necessary to require that secure encryption is applied between account information service providers, payment initiation service providers, payment service providers issuing card-based payment instruments and account servicing payment service providers when exchanging data.

27. To improve user confidence and ensure strong customer authentication, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall identify themselves to account servicing payment service providers using a form of identification issued by an independent third party. Where relevant, the use of electronic identification means and trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust service for electronic transactions in the internal market, as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 as came into force on IP completion day as defined in the EU (Withdrawal Agreement) Act 2020, should be taken into account, in particular with regard to notified electronic identification schemes.

20. Each account servicing payment service provider with payment accounts that are accessible online should offer at least one access interface enabling secure communication with account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. The interface should enable the account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments to identify themselves to the account servicing payment service provider. It should also allow account information service providers and payment initiation service providers to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user. FCA 2021/45 To ensure technology and business model neutrality, the account servicing payment service providers should be free to decide whether to offer an interface that is dedicated to the communication with account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments, or to allow, for that communication, the use of the interface for the identification and communication with the account servicing payment service providers' payment service users.

21. In order to allow account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments to develop their technical solutions, the technical specification of the interface should be adequately documented and made publicly available. The effect of Articles 30(3) and (5) is that the account servicing payment service provider should offer a facility enabling the payment service providers to test the technical solutions

at least six months prior to by FCA 2021/45 the date on which the interface will be launched to the market. To ensure the interoperability of different technological communication solutions, the interface should use standards of communication which are developed by international standardisation organisations.

22. The quality of the services provided by account information service providers and payment initiation service providers will depend on the proper functioning of the interfaces put in place or adapted by account servicing payment service providers. It is therefore important that in case of non-compliance of such interfaces with the provisions included in these Standards, measures are taken to guarantee business continuity for the benefit of the

users of those services. It is the responsibility of the FCA to ensure that account information service providers and payment initiation service providers are not blocked or obstructed in the provision of their services.

23. Where access to payment accounts is offered by means of a dedicated interface, in order to ensure the right of payment service users to make use of payment initiation service providers and of services enabling access to account information, as provided for in the Payment Services Regulations 2017 (SI 2017/752), it is necessary to require that dedicated interfaces have the same level of availability and performance as the interface available to the payment service user. Account servicing payment service providers should also define transparent key performance indicators and service level targets for the availability and performance of dedicated interfaces that are at least as stringent as those for the interface used for their payment service users. Those interfaces should be tested by the payment service providers who will use them, and should be stress-tested and monitored by the FCA.

24. To ensure that payment service providers who rely on the dedicated interface can continue to provide their services in case of problems of availability or inadequate performance, it is necessary to provide, subject to strict conditions, a fallback mechanism that will allow such providers to use the interface that the account servicing payment service provider maintains for the identification of, and communication with, its own payment service users. Certain account servicing payment service providers will be exempted from having to provide such a fallback mechanism through their customer-facing interfaces where the FCA establishes that the dedicated interfaces comply with specific conditions that ensure unhampered competition. In the event that the exempted dedicated interfaces fail to comply with the required conditions, the granted exemptions shall be revoked by the FCA.

25. In order to allow the FCA to effectively supervise and monitor the implementation and management of the communication interfaces, the account servicing payment service providers should make a summary of the relevant documentation available on their website, and provide, upon request, the FCA with documentation of the solutions in case of emergencies. The account servicing payment service providers should also make publicly available the statistics on the availability and performance of that interface.

26. In order to safeguard the confidentiality and the integrity of data, it is necessary to ensure the security of communication sessions between account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. It is in particular necessary to require that secure encryption is applied between account information service providers, payment initiation service providers, payment service providers issuing card-based payment instruments and account servicing payment service providers when exchanging data.

27. To improve user confidence and ensure strong customer authentication, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall identify themselves to account servicing payment service providers using a form of identification issued by an independent third party. Where relevant, the use of electronic identification means and trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust service for electronic transactions in the internal market, as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 as came into force on IP completion day as defined in the EU (Withdrawal Agreement) Act 2020, should be taken into account, in particular with regard to notified electronic identification schemes.

21. In order to allow account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments to develop their technical solutions, the technical specification of the interface should be adequately documented and made publicly available. The effect of Articles 30(3) and (5) is that the account servicing payment service provider should offer a facility enabling the payment service providers to test the technical solutions

22. The quality of the services provided by account information service providers and payment initiation service providers will depend on the proper functioning of the interfaces put in place or adapted by account servicing payment service providers. It is therefore important that in case of non-compliance of such interfaces with the provisions included in

1

these Standards, measures are taken to guarantee business continuity for the benefit of the users of those services. It is the responsibility of the FCA to ensure that account information service providers and payment initiation service providers are not blocked or obstructed in the provision of their services.

23. Where access to payment accounts is offered by means of a dedicated interface, in order to ensure the right of payment service users to make use of payment initiation service providers and of services enabling access to account information, as provided for in the Payment Services Regulations 2017 (SI 2017/752), it is necessary to require that dedicated interfaces have the same level of availability and performance as the interface available to the payment service user. Account servicing payment service providers should also define transparent key performance indicators and service level targets for the availability and performance of dedicated interfaces that are at least as stringent as those for the interface used for their payment service users. Those interfaces should be tested by the payment service providers who will use them, and should be stress-tested and monitored by the FCA.
24. To ensure that payment service providers who rely on the dedicated interface can continue to provide their services in case of problems of availability or inadequate performance, it is necessary to provide, subject to strict conditions, a fallback mechanism that will allow such providers to use the interface that the account servicing payment service provider maintains for the identification of, and communication with, its own payment service users. Certain account servicing payment service providers will be exempted from having to provide such a fallback mechanism through their customer-facing interfaces where the FCA establishes that the dedicated interfaces comply with specific conditions that ensure unhampered competition. In the event that the exempted dedicated interfaces fail to comply with the required conditions, the granted exemptions shall be revoked by the FCA.
25. In order to allow the FCA to effectively supervise and monitor the implementation and management of the communication interfaces, the account servicing payment service providers should make a summary of the relevant documentation available on their website, and provide, upon request, the FCA with documentation of the solutions in case of emergencies. The account servicing payment service providers should also make publicly available the statistics on the availability and performance of that interface.
26. In order to safeguard the confidentiality and the integrity of data, it is necessary to ensure the security of communication sessions between account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. It is in particular necessary to require that secure encryption is applied between account information service providers, payment initiation service providers, payment service providers issuing card-based payment instruments and account servicing payment service providers when exchanging data.
27. To improve user confidence and ensure strong customer authentication, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall identify themselves to account servicing payment service providers using a form of identification issued by an independent third party. Where relevant, the use of electronic identification means and trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust service for electronic transactions in the internal market, as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 as came into force on IP completion day as defined in the EU (Withdrawal Agreement) Act 2020, should be taken into account, in particular with regard to notified electronic identification schemes.

24. To ensure that payment service providers who rely on the dedicated interface can continue to provide their services in case of problems of availability or inadequate performance, it is necessary to provide, subject to strict conditions, a fallback mechanism that will allow such providers to use the interface that the account servicing payment service provider maintains for the identification of, and communication with, its own payment service users. Certain account servicing payment service providers will be exempted from having to provide such a fallback mechanism through their customer-facing interfaces where

the FCA establishes that the dedicated interfaces comply with specific conditions that ensure unhampered competition. In the event that the exempted dedicated interfaces fail to comply with the required conditions, the granted exemptions shall be revoked by the FCA.

25. In order to allow the FCA to effectively supervise and monitor the implementation and management of the communication interfaces, the account servicing payment service providers should make a summary of the relevant documentation available on their website, and provide, upon request, the FCA with documentation of the solutions in case of emergencies. The account servicing payment service providers should also make publicly available the statistics on the availability and performance of that interface.

26. In order to safeguard the confidentiality and the integrity of data, it is necessary to ensure the security of communication sessions between account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. It is in particular necessary to require that secure encryption is applied between account information service providers, payment initiation service providers, payment service providers issuing card-based payment instruments and account servicing payment service providers when exchanging data.

27. To improve user confidence and ensure strong customer authentication, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall identify themselves to account servicing payment service providers using a form of identification issued by an independent third party. Where relevant, the use of electronic identification means and trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust service for electronic transactions in the internal market, as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 as came into force on IP completion day as defined in the EU (Withdrawal Agreement) Act 2020, should be taken into account, in particular with regard to notified electronic identification schemes.

25. In order to allow the FCA to effectively supervise and monitor the implementation and management of the communication interfaces, the account servicing payment service providers should make a summary of the relevant documentation available on their website, and provide, upon request, the FCA with documentation of the solutions in case of emergencies. The account servicing payment service providers should also make publicly available the statistics on the availability and performance of that interface.

26. In order to safeguard the confidentiality and the integrity of data, it is necessary to ensure the security of communication sessions between account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. It is in particular necessary to require that secure encryption is applied between account information service providers, payment initiation service providers, payment service providers issuing card-based payment instruments and account servicing payment service providers when exchanging data.

27. To improve user confidence and ensure strong customer authentication, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall identify themselves to account servicing payment service providers using a form of identification issued by an independent third party. Where relevant, the use of electronic identification means and trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust service for electronic transactions in the internal market, as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 as came into force on IP completion day as defined in the EU (Withdrawal Agreement) Act 2020, should be taken into account, in particular with regard to notified electronic identification schemes.

26. In order to safeguard the confidentiality and the integrity of data, it is necessary to ensure the security of communication sessions between account servicing payment service providers, account information service providers, payment initiation service providers and

payment service providers issuing card-based payment instruments. It is in particular necessary to require that secure encryption is applied between account information service providers, payment initiation service providers, payment service providers issuing card-based payment instruments and account servicing payment service providers when exchanging data.

27. To improve user confidence and ensure strong customer authentication, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall identify themselves to account servicing payment service providers using a form of identification issued by an independent third party. Where relevant, the use of electronic identification means and trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust service for electronic transactions in the internal market, as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 as came into force on IP completion day as defined in the EU (Withdrawal Agreement) Act 2020, should be taken into account, in particular with regard to notified electronic identification schemes.

27. To improve user confidence and ensure strong customer authentication, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall identify themselves to account servicing payment service providers using a form of identification issued by an independent third party. Where relevant, the use of electronic identification means and trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust service for electronic transactions in the internal market, as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 as came into force on IP completion day as defined in the EU (Withdrawal Agreement) Act 2020, should be taken into account, in particular with regard to notified electronic identification schemes.